Mirasys Administrator Guide

V9.6

English version published on 3 July 2023

Mirasys Oy – Espoo, Finland

Tel +358 (0)9 2533 3300 • Email info@mirasys.com • www.mirasys.com

documentation.mirasys.com • training.mirasys.com

Table of content

Mirasys VMS Admin Guide

System Administration

Overview of This Guide

This guide is intended for those who set up a Mirasys system.

It shows how to add servers to the system and change their settings, add user accounts and user profiles, and monitor the system.

Technical Support

For technical support and warranty issues, please contact the system supplier.

What is the Mirasys VMS software?

Mirasys software is a distributed digital video management system (VMS or DVMS) for video and audio surveillance applications.

The software can monitor real-time and recorded video, audio and text data and control PTZ cameras, I/O devices, and IP cameras.

The software supports systems consisting of analogue or digital surveillance cameras, supporting the creation of analogue, digital or hybrid (consisting of both analogue and digital) surveillance systems.

A centralized surveillance system domain can consist of up to 150 local or remote VMS Servers.

Mirasys software is sold separately and part of Mirasys video management systems consisting of both the software and the VMS Server hardware.

Please contact your Mirasys supplier for information on Mirasys software or hardware.

What does a System Contain?

The Mirasys system consists of these components:

- 1-150 VMS Servers
  - **Master Server** (dedicated server – recommended -, one of the video recording VMS Servers, or the only server in a single-server, non-networked environment)
  - **VMS Server** ("recording servers" if the system consists of multiple servers)
- Client applications:
  a. Mirasys System Manager
  b. Mirasys Spotter
  c. Mirasys Spotter Web
  d. Mirasys Spotter Mobile

VMS Servers

The VMS servers record video and audio from multiple cameras and audio channels and write the data to a storage device.

You can access a VMS Server locally or over a network using the System Manager and Spotter programs and monitor server functionality through the Spotter Diagnostics plugin.

A server is a computer with storage, the Windows operating system, and the installed VMS software with required drivers.

Several devices can be connected to a VMS Server:

- PTZ (dome) cameras and keyboards
- External devices, such as sensors, to the digital inputs
- External devices, such as doors, lights, and gates, connected to digital outputs
- Special integrated devices like radar, IoT device or 3rd party system
- Storage or backup unit (NAS, SAN, or RAID, for example)

Master Server

In a networked system, one of the servers must be set as the Master Server.

A Master Server is the central server of a surveillance system.

All other VMS Servers connect to it, and all client applications communicate through the Master Server.

If the system contains only one server, then that server is the Master Server.

If there is more than one server, the Master Server can be set freely.

It is recommended that the Master Server is a dedicated server for this purpose alone in a more extensive system.

NOTE: Master Servers must have *SQL Server Express 2014* or other *Microsoft SQL Server 2014* installed.

The Master Server does these things:

1. It verifies the identity of all programs and users who try to log on to the system (authentication).

- It stores all system configuration data.
- It stores all user data.
- It monitors the system.
- It synchronizes the clocks on all servers.
- It generates reports.
- It stores watchdog events.
- It stores alarms.
- It stores audit trails.

Client Programs

System administrators use the **System Manager** program for these tasks:

- Configuring the servers.
- Adding user accounts and user profiles.
- Monitoring the system.

System operators use the **Spotter** application for:

1. Monitor real-time and recorded video and audio
2. Control digital I/O switches and PTZ cameras
3. Export video and audio clips to local media
4. Receive and handle alarm notifications
5. Create video matrixes via the optional, separately sold Agile Video Matrix (AVM) software
6. Use other plugins like Grafana reporting or list management

Network Requirements

The network requirements apply to systems where users access the servers over a network.

OS Compatibility

Mirasys VMS V9 supports the following operating systems:

Operating System	**Server with analogue camera support via capture cards**	**Server with only IP cameras or connected video servers (encoders)**	**Gateway server**	**System Manager application**	**Spotter application**
Windows 10	-	X	X	X	X
Windows 11	-	X	X	X	X
Windows Server 2016	-	X	X	X	X
Windows Server 2019	-	X	X	X	X
Windows Server 2022	-	X	X	X	X

Make sure that the “Desktop Experience” and “Media Foundation” features is activated for Windows server operating systems.

Configuring the System

After connecting the cameras and other devices to the servers, configure the system settings and add user accounts and user profiles.

To configure the system, perform these steps:

- Add servers to the system and configure their settings.
- Add the correct licenses for the servers.
- Add IP cameras and other IP devices.
- Add user profiles.
- Add user accounts.

Note: *Install the client programs on each computer used to access the system over a network.*

A separate "Spotter only" installer is provided.

Note: *After configuring the system,* ***back up system settings and all VMS Server settings*** *on the* ***System*** *tab.This way, you can restore the settings, for example, if a hard disk fails.*

Log In

This section describes how to log in and log off from System Manager.

Only system administrators or users with monitoring rights are allowed to log in to System Manager.

Logging in

User credentials

Default username and password

Username: Admin

Password: 0308

The default username and password should not be used even in closed networks.

Please ensure that the default username and password are not in use after installing the system.

How to log in

To login to System Manager:

Do one of the following:

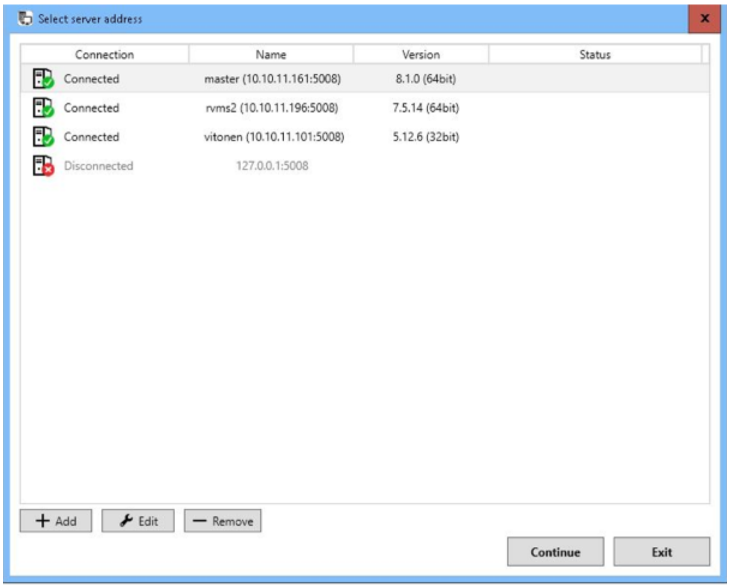
1. Double-click the shortcut icon **System Manager** on the desktop.
2. Click **Start**, point to **Programs,** and then to **DVMS**. Click **System Manager**.

In systems that have only one Master Server address configured, the System Manager login screen is shown.

In systems with multiple masters and addresses configured, or if the user presses the “Delete” key in the initial startup phase, the site selection screen is shown.

The user can add, remove or edit Master Server addresses or choose a server to log on on this screen.

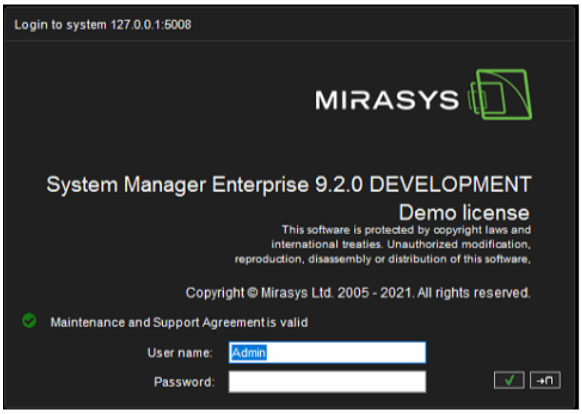
After selecting a server and pressing the “Continue” button, a user is taken to the login screen.



Select server address

Connection	Name	Version	Status
Connected	master (10.10.11.161:5008)	8.1.0 (64bit)	
Connected	rvms2 (10.10.11.196:5008)	7.5.14 (64bit)	
Connected	vitonen (10.10.11.101:5008)	5.12.6 (32bit)	
Disconnected	127.0.0.1:5008		

On the login screen, type your username in the **Username** box and your password in the **Password** field.



Login to system 127.0.0.1:5008

MIRASYS

System Manager Enterprise 9.2.0 DEVELOPMENT

Demo license

This software is protected by copyright laws and international treaties. Unauthorized modification, reproduction, disassembly or distribution of this software.

Copyright © Mirasys Ltd. 2005 - 2021. All rights reserved.

✓ Maintenance and Support Agreement is valid

User name: Admin

Password:

Note: *The username and password are case-sensitive.*

Click **OK**. A progress bar is shown on the screen while the program loads.

After the program starts, the user interface is shown. To **log off** or to **change the user** click on the menu bar **File** and then **Log off. To quit** the program**:**

- On the menu bar, click **File** and then **Exit**.
- Close the application window.

Note: The user can only have one System Manager application running at any one time.

It is not possible to have the System Manager simultaneously connected to multiple servers.

To connect to another Master Server, exit from the current Master and choose another Master Server from the site selection screen.

Locking System Manager

You can manually lock the program to protect it, for example, when you go away from your desk.

To lock the program, do one of the following:

1. On the menu bar, click **File** and then **Lock Program**.
2. On the status bar, click **Lock program**.

To unlock the program:

- After locking the program, the login screen is shown.
    a. Type the user name in the **User name** box and the password in the **Password** box.

Note: *The password is case sensitive.*

Management User Interface

The System Manager User interface

The System Manager User Interface contains these elements:

Menu bar.

- **File**
- **Log Off**
- **Lock Program**
- **Import**
- **Export**

Maintenance

Set maintenance state on to control the failover transition state off.

Help

About

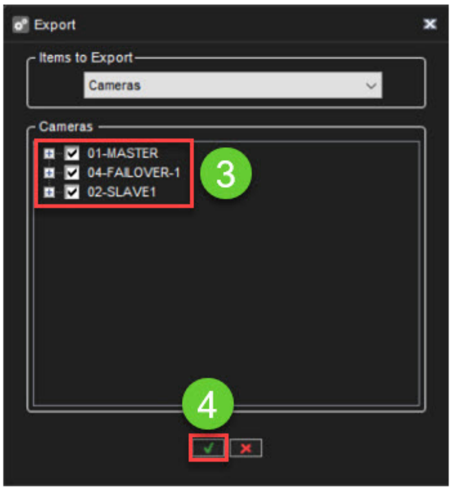
to see information about the program version.

and then **Help Topics** to use the online guide.

Exporting system camera information to the CSV

1. Click **File**
2. Click **Export**

3. Select the servers
4. Click **OK**

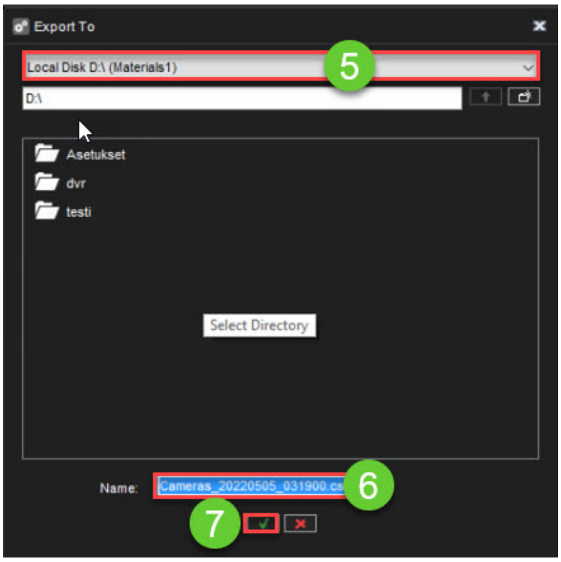


Export

Items to Export: Cameras

Cameras
☑ 01-MASTER
☑ 04-FAILOVER-1
☑ 02-SLAVE1

1. Select the location
2. Enter the name of the export
3. Click **OK**



Export To

Local Disk D:\ (Materials1)

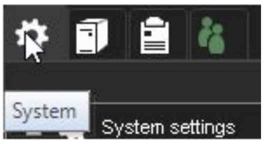
D:\

Asetukset
dvr
testi

Select Directory

Name: Cameras_20220505_031900.cs

System



You can edit and backup system settings on the System tab, monitor the system and examine diagnostic information about the course.

You can also change license keys for servers on this tab, such as adding more camera channels and installing a new IP camera, metadata, and client plugin drivers.

Also, you can configure the software watchdog.

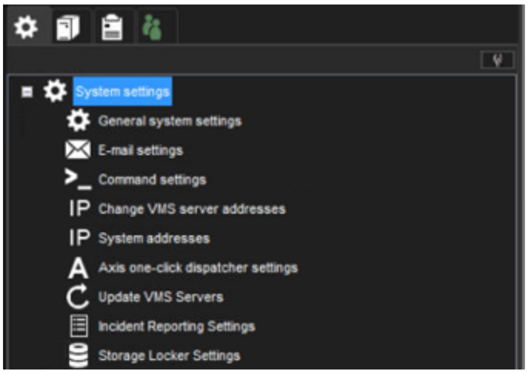
The tab contains these tools:

1. System settings
2. General system settings
3. E-mail settings
4. Command settings
5. Change VMS server addresses
6. System addresses
7. Update VMS Servers
8. Backup
9. Export logs
10. Backup settings
11. Restore settings
12. Monitoring
13. SM Server diagnostics
14. Local recorder diagnostics
15. Licenses
16. Watchdog
17. Watchdog settings
18. Watchdog logs
19. Add-ins
20. Install driver
21. Install metadata driver
22. Install client driver
23. Install client plugin

To open a tool, do one of the following:

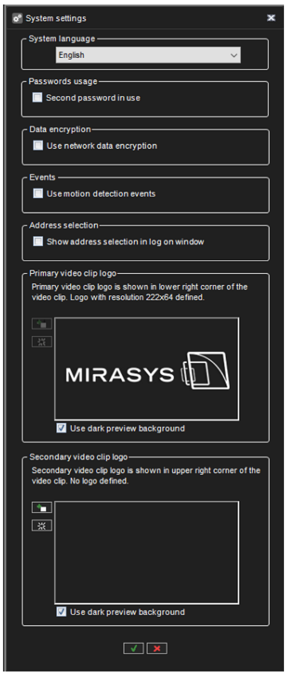
- Click the tool and then click Edit 🔧
- Double-click the tool**.**
- Drag the tool from the **System** tab to the workspace

System settings



- System settings
  - General system settings
  - E-mail settings
  - Command settings
  - Change VMS server addresses
  - System addresses
  - Axis one-click dispatcher settings
  - Update VMS Servers
  - Incident Reporting Settings
  - Storage Locker Settings

General System Settings



System settings

System language: English

Passwords usage
□ Second password in use

Data encryption
□ Use network data encryption

Events
□ Use motion detection events

Address selection
□ Show address selection in log on window

Primary video clip logo
Primary video clip logo is shown in lower right corner of the video clip. Logo with resolution 222x64 defined.
☑ Use dark preview background

Secondary video clip logo
Secondary video clip logo is shown in upper right corner of the video clip. No logo defined.
☑ Use dark preview background

In this section, you can control the following:

- System language

- The password usage

It is possible to configure the system to require two separate passwords for all users.

This is done by activating the “Second password in use” option in general system settings.

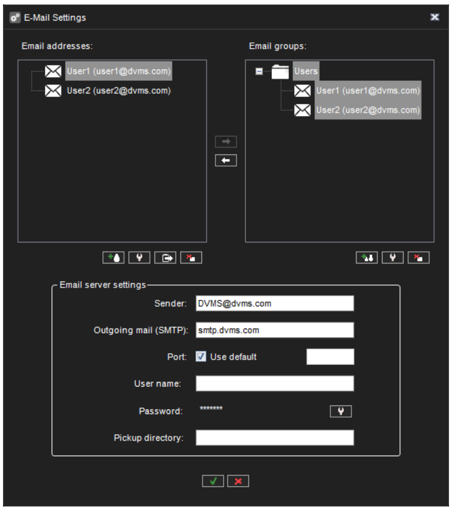
When this mode is selected, all users are required to give two passwords.

The default second password is empty. This feature allows limiting that no single person can review videos alone.

If one password is known to one person and the other password is known to another person, both persons must be present when reviewing videos.

- Data encryption
- Events(the setting for sending motion information to clients)
- Address selection
- Primary video clip logo(Logos that are attached to exported video clips)
- Secondary video clip logo(Logos that are attached to exported video clips)

E-Mail Settings


E-Mail Settings

Email addresses:
User1 (user1@dvms.com)
User2 (user2@dvms.com)

Email groups:
Users
User1 (user1@dvms.com)
User2 (user2@dvms.com)

Email server settings
Sender: DVMS@dvms.com
Outgoing mail (SMTP): smtp.dvms.com
Port: ☑ Use default
User name:
Password: *******
Pickup directory:

You can specify e-mail addresses and groups which can be defined to receive reports about events specified in the Software Watchdog.

To set the e-mail notification settings:

- On the **System** tab, open **E-mail settings**.

- Type the sender’s e-mail address into the **Sender** field. Note that some e-mail applications are configured to accept messages only from valid e-mail addresses.
- Type the name of the outgoing mail server into the **Outgoing mail (SMTP)** field. The specified server will be used for sending all e-mail notifications.
- Type the login information and port for the SMTP server into the appropriate fields.
- Set the events for which notifications will be sent as instructed in the Software Watchdog.

Note: Emails are not sent to all system email recipients.

The administrator can control which Watchdog events and alarms to which email recipients or groups the email is sent.

To add new e-mail addresses to the system:

- On the **System** tab, open **E-mail settings**.
- Click **Add new e-mail address** to add a new address.

- Type the recipient’s name and e-mail address into the **Name** and **Address** fields.
- Click **OK**.

To add a new e-mail group to the system:

- On the **System** tab, open **E-mail settings**.
- Click **Add new e-mail address** to add a new address.

- Type the group name
- Click **OK**.

To add one or more recipients to a group:

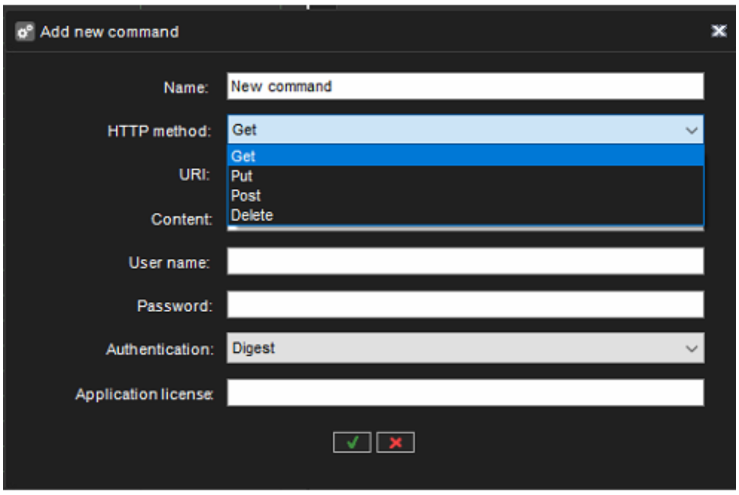
1. Highlight the desired group on the group list
2. Highlight the desired recipient(s) in the recipient list
3. Click on the arrow to add the selected recipients to the selected group

Other available actions:

🔧	Editing email names, addresses, and group names and removing persons from groups is possible with the edit buttons.
←	Persons can be removed from groups with the arrow.
✖	Persons and groups can be removed with the button.
➡	Test email can be sent with a button to a selected email address using the settings defined in the email settings dialogue.

Command Settings

Command settings are used for HTTP command sending


Add new command

Name: New command

HTTP method: Get

URI:

Content:

User name:

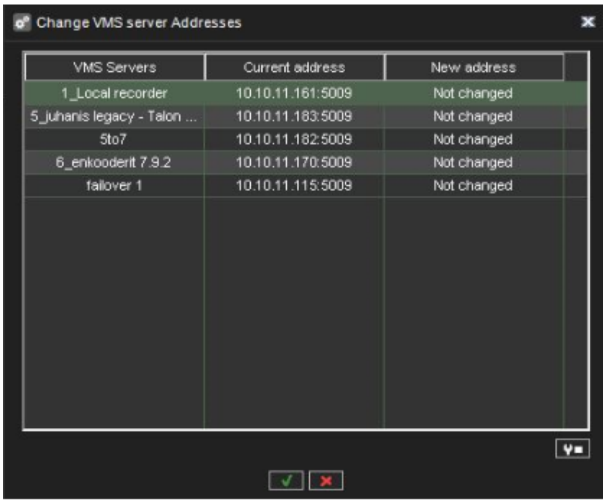
Password:

Authentication: Digest

Application license:

Change VMS Server Addresses

If the IP address or DNS name of a server changes, you can define the new address/name through the **Change VMS Server addresses** tool.



VMS Servers	Current address	New address
1_Local recorder	10.10.11.161:5009	Not changed
5_juhanis legacy - Talon ...	10.10.11.183:5009	Not changed
5to7	10.10.11.182:5009	Not changed
6_enkooderit 7.9.2	10.10.11.170:5009	Not changed
failover 1	10.10.11.115:5009	Not changed

To change a server's IP address or DNS name:

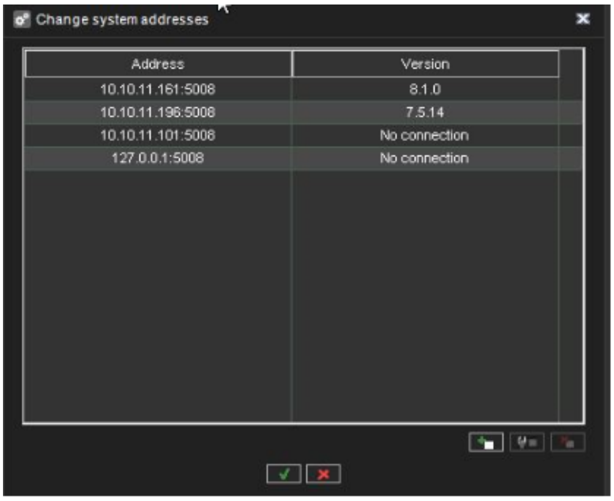
1. On the **System** tab, open **Change VMS Server addresses**.
2. Click on the name of the server with the changed IP address.
3. Click **Change VMS Server address**

4. Type the new IP address or DNS name of the server into the **New VMS Server address** field.
5. Click **OK**.

System Addresses

A Master Server is the central server of a surveillance system.

All other VMS Servers connect to it, and all client applications communicate through the Master Server. During the login phase, the client applications can select the Master Server they will connect to.



Change system addresses

Address	Version
10.10.11.161:5008	8.1.0
10.10.11.196:5008	7.5.14
10.10.11.101:5008	No connection
127.0.0.1:5008	No connection

You can define multiple Master Server addresses that the client applications can connect to. The addresses can be provided as IP addresses (e.g. *http://195.168.0.1*) or DNS names (e.g. http://www.example.com).

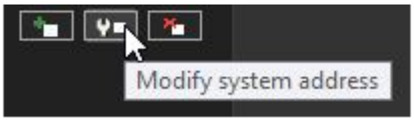
Note: *Users can connect to any of the defined Master Server addresses provided they have a compatible username and password for the Master Server.*

To add a Master Server address:

1. On the **System** tab, open **System addresses**
2. Click **Add new system address**.
3. Type the new system address (either IP address or DNS name) to the **Add** field.
4. Click **OK**.

To edit a Master Server address:

1. On the **System** tab, open **System addresses**.
2. Click on the Master Server address with the changed IP address.



3. Click Modify system address .
4. Type the new IP address or DNS name of the DVR into the **Modify system address** field.
5. Click **OK**.

To remove a Master Server address:

- On the **System** tab, open **System addresses**.
- Click on the Master Server address you want to remove.
- Click **Remove system address**.

Axis one-click dispatcher settings

Installation steps

Install the O3C-server as described in the guide "AXIS O3C Server Reference. Windows and Linux Versions" (Technical Reference Document. AXIS One-Click Cloud Connection Server 2.30.0), part 2.2.2.

Important things:

- Install the O3C-server as described in the guide "AXIS O3C Server Reference. Windows and Linux Versions" (Technical Reference Document. AXIS One-Click Cloud Connection Server 2.30.0), part 2.2.2.

Important things:

- setup provider certificate authority:

Directory in which the CA should be set up [default: ca]: (by default ca)

Passphrase for the CA key (DO NOT FORGET THIS!) [default: N/A]: pAs_sw!ord (some password)

Valid time, in days [default: 7300]: 100 (any number)

Issue a server certificate:

Path to the CA directory [default: ca]: (as above)

Passphrase for the CA key [default: N/A]: pAs_sw!ord (as above)

Subject Alternative Names (separated by comma) [default: N/A]: 172.17.102.56 (very important!!! Should be equal IP address of O3C server)

Valid time, in days [default: 398]: 100 (as above)

Result:

Concatenated server certificate and key saved to: ca/issued/stserver_EA363E5578E696E7.pem

Register O3C server as service in Windows SCM: there is needed the Power Shell tool for Windows! And for install call:

```
.\setup_service.ps1 add -c C:\o3c-server\o3c-server.conf
```

Configure o3c-server.conf

listen_client = 172.17.102.56:80

IP and port where the server will wait for the client (the camera) connections

stserverid = test_o3c_server

Any string

cert_file = C:\o3c-server\stserver_EA363E5578E696E7.pem issued server certificate created after command: "pkitool issue-server-cert"

provider_ca = C:\o3c-server\stserver_ca.crt

CA certificate from ca directory created after the command: "pkitool setup-provider-ca"

provider_name =

can be left blank

credentials = root:root

for device access requests

O3C-server service

By default, the service is called Axis O3C Server in Services or O3C-server in command prompt.

1. Start the O3C-server service
2. Enable One-click technology on the camera as described in the 4.1 part of the guide.
3. Disable firewalls or add O3C-server to the exceptions
4. Register the camera as described in guide 4.2 part.
    a. http://172.17.102.56/admin/dispatch.cgi?action=register&user=adp_mirasys_100&pass=GQ41lSRbbEb4w3sorkN8&mac=B8A44F17AAFA&oak=8A22D6434817&server=172.17.102.56:80
    b. where:user=adp_mirasys_100, pass=GQ41lSRbbEb4w3sorkN8 - Mirasys credentials (Provider name and password) from Axismac=B8A44F17AAFA, oak=8A22D6434817 - MAC address and OAK key from the camera
    c. To find the MAC address using the following string in the browser: http://172.17.100.84/axis-cgi/admin/param.cgi?action=list&group=Network
    d. server=172.17.102.56:80 - as "listen_client" in o3c-server.conf
5. Check that the camera was connected to the O3C-server: call in the browser th string: http://172.17.102.56:80/admin/status.cgi 172.17.102.56 - IP address of O3C-server
6. And check that there is a comment about the connected client as follows: "id=4.b8a44f17aafa srcaddr=172.17.100.84:34148 accepted=1 v=2 rx=0 tx=0 connected=2022-01-10T12:45:40.875571Z

Total number of clients: 1"

PS: the camera tries to connect to the server every 20 seconds

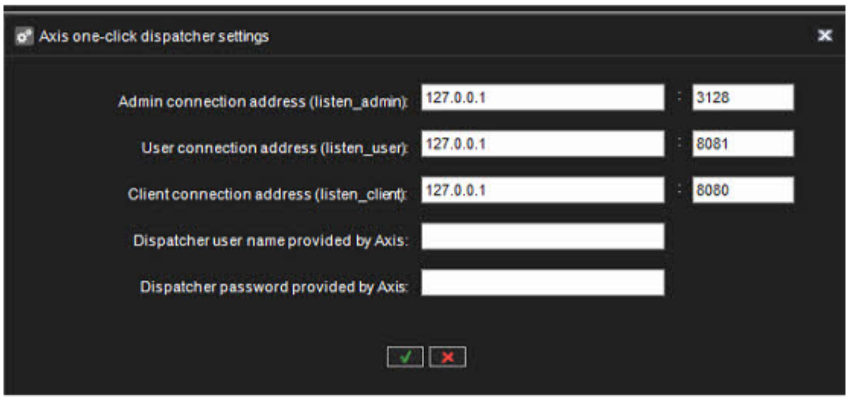
1. Check that we can get options from the camera: for that, it needed to configure the proxy settings for browser -
2. Open system Internet Options
3. Select Connections tab -> Select LAN settings button -> to enable "Use a proxy server for LAN (...)" and input the proxy IP address and port. (in the current case there is a local IP address and port 80)
4. After that we can get the camera capabilities in the browser:
    a. http://b8a44f17aafa/axis-cgi/param.cgi?action=list&group=root.RemoteService where b8a44f17aafa - MAC address of the camera

Filter for wireshark for Axis P1375:

```
((ip.src == 172.17.100.84) && (ip.dst == 172.17.102.56)) || ((ip.src == 172.17.102.56) && (ip.dst == 172.17.100.84))
```

Add Axis One-Click Camera

- Open **System tab**
- Go to **System Settings** and open **Axis one-click dispatcher settings**
- Enter all necessary details and click **OK**



Axis one-click dispatcher settings

Admin connection address (listen_admin): 127.0.0.1 : 3128

User connection address (listen_user): 127.0.0.1 : 8081

Client connection address (listen_client): 127.0.0.1 : 8080

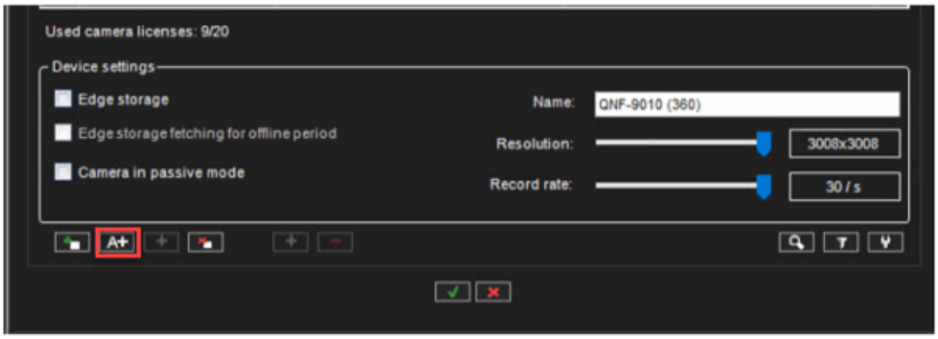
Dispatcher user name provided by Axis:

Dispatcher password provided by Axis:

4. Open the **VMS Servers tab**

5. Click **Hardware**

6. Click **Add Axis One-Click Camera** icon


Used camera licenses: 9/20

Device settings

□ Edge storage

□ Edge storage fetching for offline period

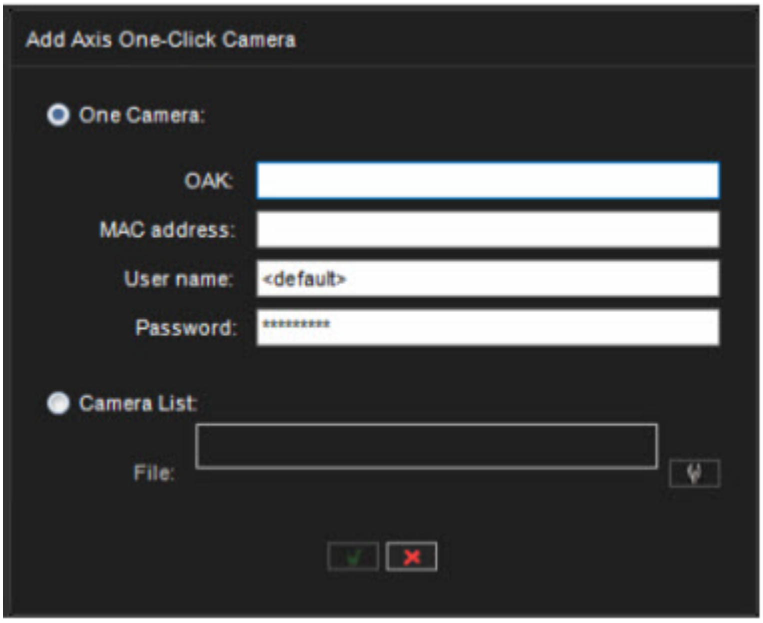
□ Camera in passive mode

Name: QNF-9010 (360)

Resolution: 3008x3008

Record rate: 30 / s

7. Enter Axis One-Click Camera details and click **OK**


Add Axis One-Click Camera

● One Camera:

OAK:

MAC address:

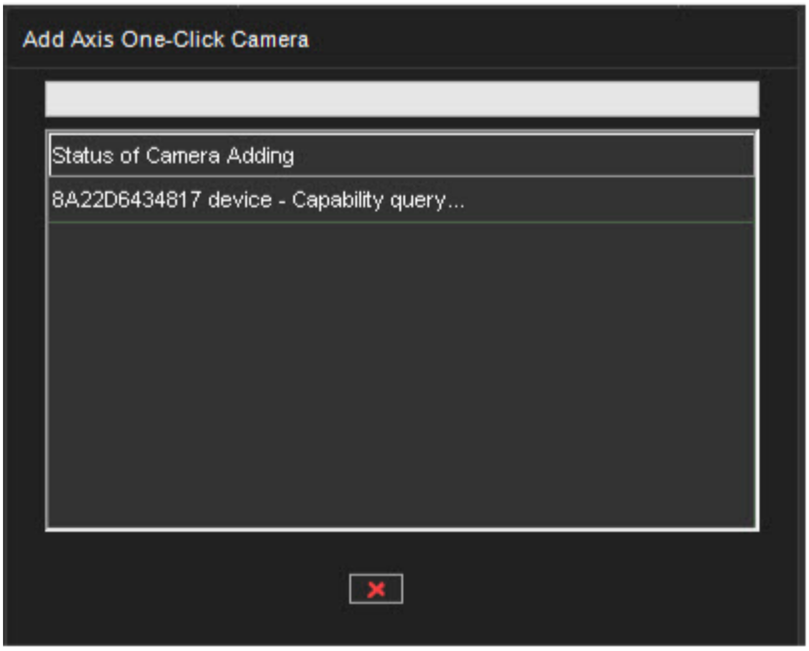
User name: <default>

Password: *********

○ Camera List:

File:

After clicking the OK, the camera query starts



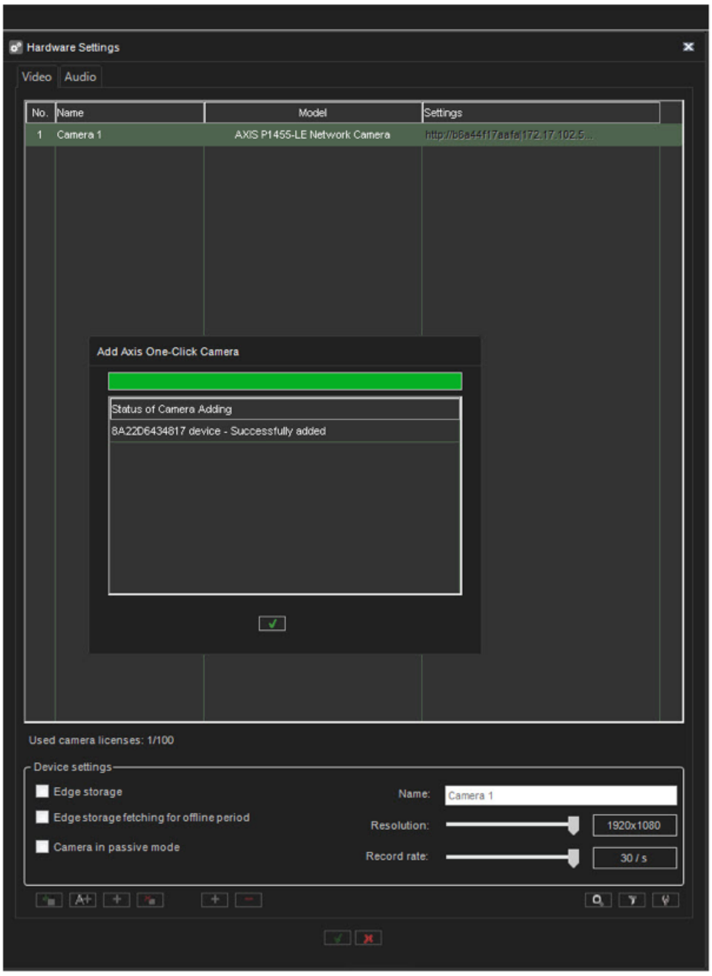
Add Axis One-Click Camera

Status of Camera Adding

8A22D6434817 device - Capability query...

When the camera query is finished, the device will be added to the hardware list

8. Click **OK** to finalize



Hardware Settings

No.	Name	Model	Settings
1	Camera 1	AXIS P1455-LE Network Camera	http://b8a44f17aafa|172.17.102.5...

Add Axis One-Click Camera

Status of Camera Adding
8A22D6434817 device - Successfully added

Used camera licenses: 1/100

Device settings

□ Edge storage

□ Edge storage fetching for offline period

□ Camera in passive mode

Name: Camera 1

Resolution: 1920x1080

Record rate: 30 / s

Update VMS Servers

It is possible to update all connected VMS Servers remotely via the **Update VMS Servers** –option

The master server must be upgraded from the Windows **Control Panel\Programs\Programs and Features\Uninstall or change a program.**

! Please remember to set the **Maintenance state on** before upgrading.

- Click **Maintenance**
- Select **Set maintenance state on**

- Select the duration of the maintenance mode

Updating VMS servers

To update servers, first, select the installation file with the button:

🔧

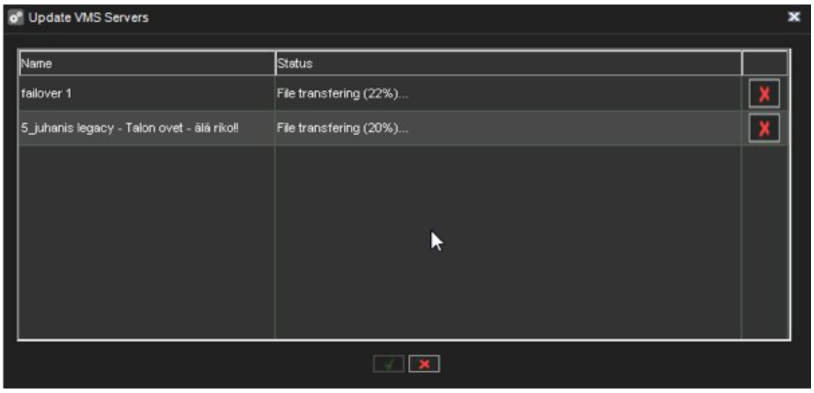
The list is updated to show which servers can be updated with the selected installation file.

Note: *When performing a major version upgrade, for example, from VMS 6. x to 7. x, it is usually necessary to first upgrade the server licenses, and only after this upgrade the VMS software.The Update VMS Servers dialogue will inform the user if a license upgrade is needed before the software update.*Next, choose which servers you want to update and if you want to perform a backup before updating.

By selecting this button

✓

you will start the update, and an update progress dialogue is shown:



Name	Status	
failover 1	File transfering (22%)...	✗
5_juhanis legacy - Talon ovet - älä riko!!	File transfering (20%)...	✗

This dialogue can be closed at any time without affecting the server updates.

Notes:

- The progress dialogue might display no status information for the installation file transfer and update progress if the network connection is slow or intermittent.
    - This is no cause for alarm; in most cases, the update will be successful, but it might take a long time (20 – 30 minutes).
    - It is recommended to prepare for the possibility to have remote access to any such servers.
- If a local server were selected to be updated, the system manager would automatically close after this dialogue is shown.
- In rare cases, some servers require system restart after remote VMS software update if the connection between the Master Server and VMS Server is not returning after the update.
    - It is recommended to monitor the connection to VMS Servers after the update.
- Since Version 7.4.3, Mirasys VMS has had support for 64-bit servers. The upgrade from 32-bit (x86) to 64-bit can be achieved precisely by installing any DVMS version.
    - After the update, the control panel of windows will show DVMS-x64 for 64-bit DVMS.

Incident Reporting Settings

From the Incident Reporting settings, the user predefines the parameters, which will be used while viewing or exporting the Incident or Daily log reports.

Company information

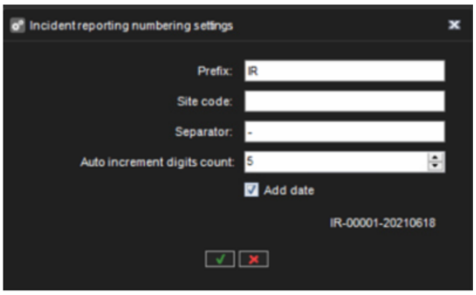
- Company name

- Company address
- Company logo

Reporting numbering

Incident Reporting numbering details:

- Prefix
- Site code
- Separator
- Autoincrement digits count



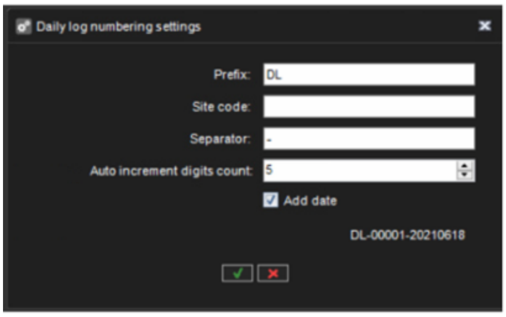
Incident reporting numbering settings

Prefix: IR
Site code:
Separator: -
Auto increment digits count: 5
☑ Add date

IR-00001-20210618

Daily log numbering details:

- Prefix
- Site code
- Separator
- Autoincrement digits count



Daily log numbering settings

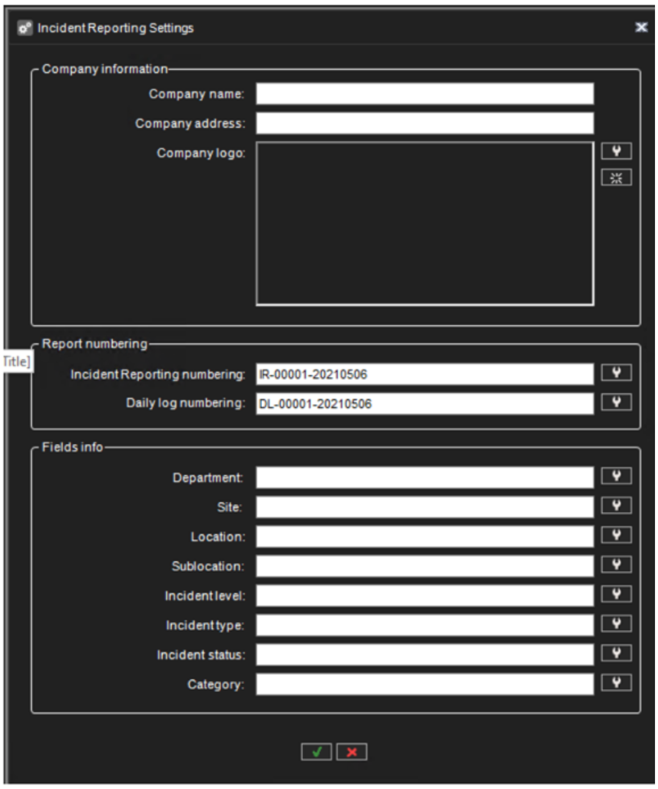
Prefix: DL
Site code:
Separator: -
Auto increment digits count: 5
☑ Add date

DL-00001-20210618

Fields info

- Department
- Site
- Location

- Sublocation
- Incident level
- Incident type
- Incident status
- Category



Incident Reporting Settings

Company information

Company name:

Company address:

Company logo:

Report numbering

Incident Reporting numbering: IR-00001-20210506

Daily log numbering: DL-00001-20210506

Fields info

Department:

Site:

Location:

Sublocation:

Incident level:

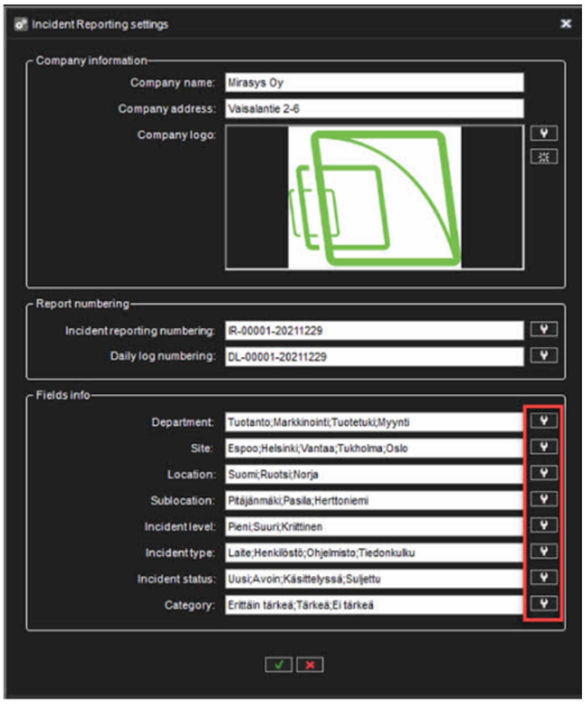
Incident type:

Incident status:

Category:

Add values

1. Select the correct field and click **Update values**



Incident Reporting settings

Company information

Company name: Mirasys Oy

Company address: Vaisalantie 2-6

Company logo:

Report numbering

Incident reporting numbering: IR-00001-20211229

Daily log numbering: DL-00001-20211229

Fields info

Department: Tuotanto;Markkinointi;Tuotetuki;Myynti

Site: Espoo;Helsinki;Vantaa;Tukholma;Oslo

Location: Suomi;Ruotsi;Norja

Sublocation: Pitäjänmäki;Pasila;Herttoniemi

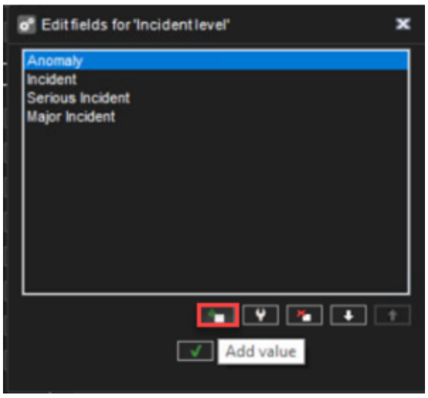
Incident level: Pieni;Suuri;Kriittinen

Incident type: Laite;Henkilöstö;Ohjelmisto;Tiedonkulku

Incident status: Uusi;Avoin;Käsittelyssä;Suljettu

Category: Erittäin tärkeä;Tärkeä;Ei tärkeä

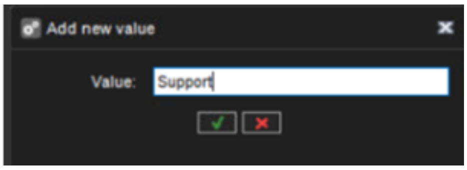
2. Click **Add value**



Edit fields for 'Incident level'

Anomaly
Incident
Serious Incident
Major Incident

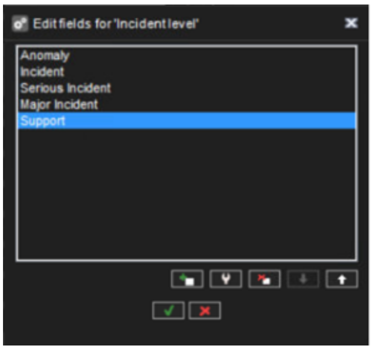
3. Enter the name of the value
4. Click **OK**



Add new value

Value: Support

5. New added value can be seen in the list

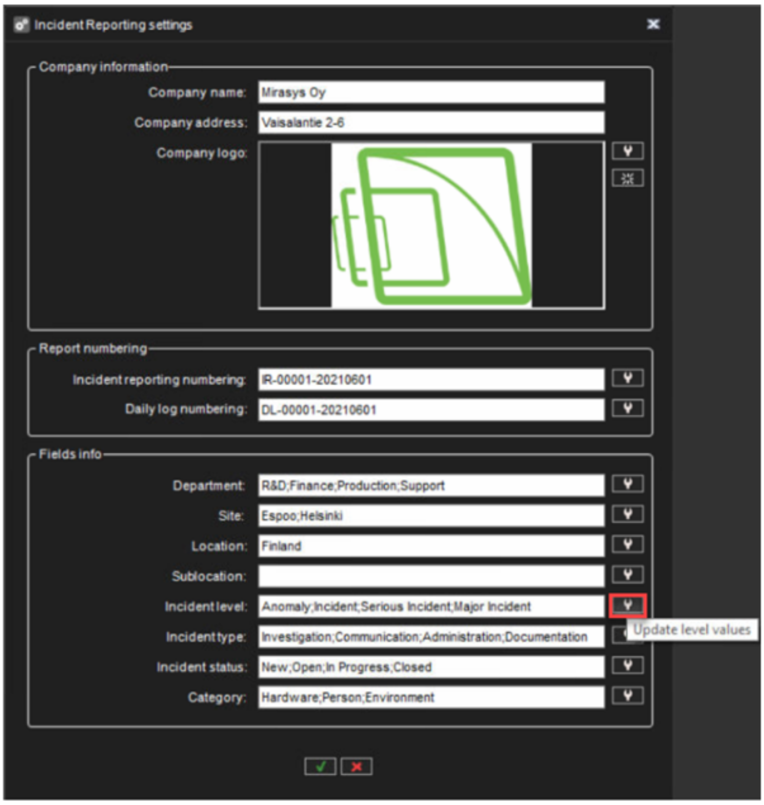


Edit fields for 'Incident level'

Anomaly
Incident
Serious Incident
Major Incident
Support

Edit values

1. Click icon **Update values**



Incident Reporting settings

Company information

Company name: Mirasys Oy

Company address: Vaisalantie 2-6

Company logo:

Report numbering

Incident reporting numbering: IR-00001-20210601

Daily log numbering: DL-00001-20210601

Fields info

Department: R&D;Finance;Production;Support

Site: Espoo;Helsinki

Location: Finland

Sublocation:

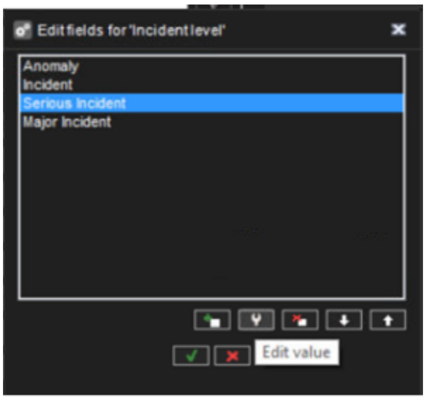
Incident level: Anomaly;Incident;Serious Incident;Major Incident

Incident type: Investigation;Communication;Administration;Documentation

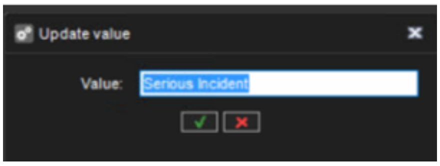
Incident status: New;Open;In Progress;Closed

Category: Hardware;Person;Environment

2. Select a value from the list and click **Edit value**

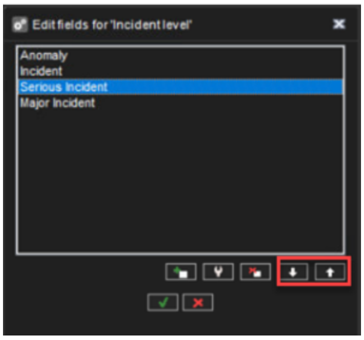


3. Enter a new value name and click **OK**



Changing the order of the values

- Select the value and click arrows to set the proper order of the values.
- Click **OK** to confirm changes



Storage Locker Settings

Storage Locker Settings contains the following values:

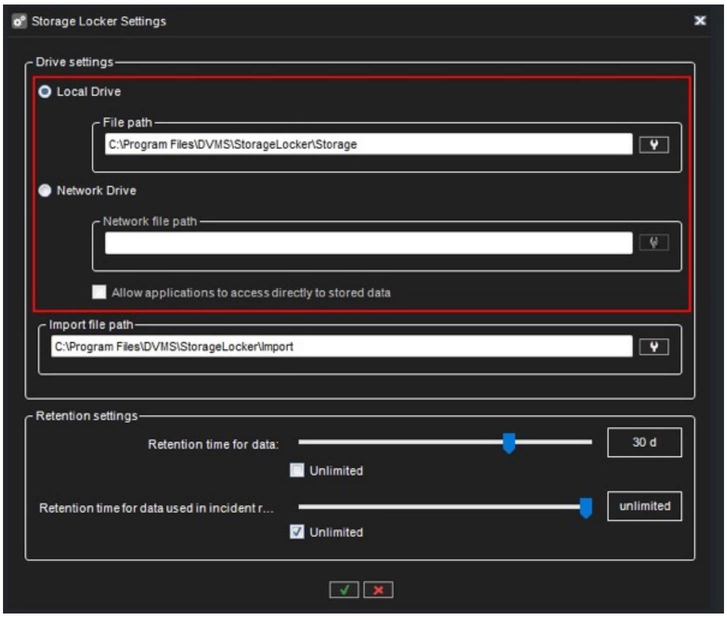
File path:

Defines the location of the Storage Locker file storage that can be either local or network disk. As the default location, Storage Locker file storage is located in the master server's local disk.

Changing the file path

Please note that old storage locker data is not copied to the new location

- Select if a local drive or network drive is used.



Storage Locker Settings

Drive settings

● Local Drive

File path: C:\Program Files\DVMS\StorageLocker\Storage

○ Network Drive

Network file path:

□ Allow applications to access directly to stored data

Import file path: C:\Program Files\DVMS\StorageLocker\Import

Retention settings

Retention time for data: 30 d

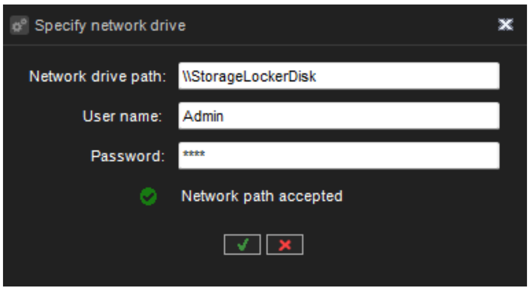
□ Unlimited

Retention time for data used in incident r... unlimited

☑ Unlimited

2. If the local drive is selected, click **Set file path for data storage.** Select a new location and click **OK.**

3. If a network drive is selected, click **Set network file path for data storage.** Specify network path, username, and password and click **OK.**



Specify network drive

Network drive path: \\StorageLockerDisk

User name: Admin

Password: ****

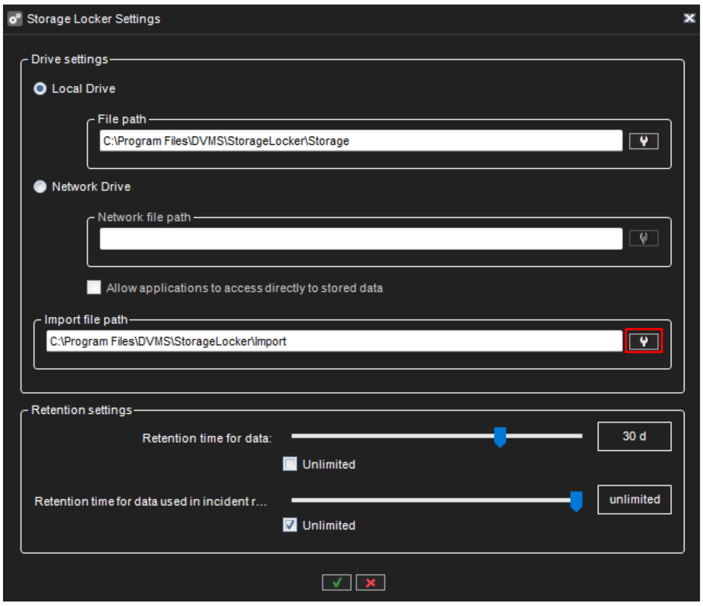
Network path accepted

When a network drive is used for Storage Locker data storage, it is possible to allow Spotter applications directly to access saved data from the network disk by checking the option **Allow applications to access directly to stored data**.

Import file path:

If someone has exports that are needed to be added to the Storage locker, those exports should be placed in a folder that is defined in Storage locker settings as "Import file path". How to use:

- Each import data need to be in its own folder, files that will be placed into the import folder directly will be ignored
- Each import folder can have several subfolders
- Images and clips can be placed in one folder, Storage locker will import them one by one
- SEF archives should be in their own folder and not mixed with other data (like images, clips, etc.)
- Import data should be copied all at once if something should be added - it should be copied with its own folder, files added to existing folders are not supported (those files will not be processed)



Storage Locker Settings

Drive settings

● Local Drive

File path: C:\Program Files\DVMS\StorageLocker\Storage

○ Network Drive

Network file path:

□ Allow applications to access directly to stored data

Import file path: C:\Program Files\DVMS\StorageLocker\Import

Retention settings

Retention time for data: 30 d

□ Unlimited

Retention time for data used in incident r... unlimited

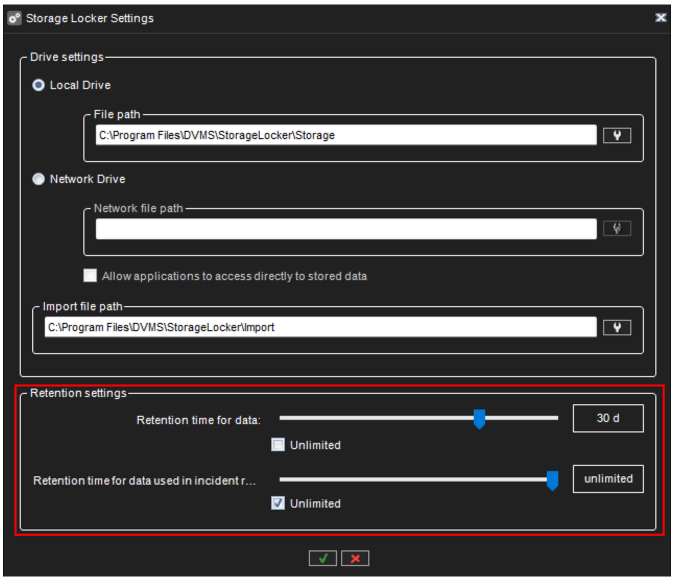
☑ Unlimited

The retention time for data

The retention time for data sets defines how long Storage Locker retains data, which are not used in any Incident Report

The retention time for data used in the incident reports

The retention time for data used in incident reports defines how long Storage Locker retains data, which are used in any Incident Report



Storage Locker Settings

Drive settings

● Local Drive

File path: C:\Program Files\DVMS\StorageLocker\Storage

○ Network Drive

Network file path:

□ Allow applications to access directly to stored data

Import file path: C:\Program Files\DVMS\StorageLocker\Import

Retention settings

Retention time for data: 30 d

□ Unlimited

Retention time for data used in incident r... unlimited

☑ Unlimited

List Management settings

List management makes it possible to define identities and lists so that the allowed or not allowed identities can be defined.

The settings define and manage identity and list management settings. Settings allow you to:

- Add, edit, and delete identities containing license plates and face images
- Add, edit, and delete lists and manage list content
- Import and export lists and identities
- Configure LPR and FR event database retention limits
- Enable and define integration and its settings

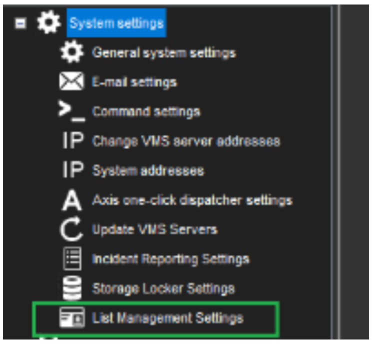
The System manager application provides several dialogs to access and modify list management service data and settings. The dialogs can be found in the “System settings“ section.

> Integration requires LPR and FR integration license.

List Management Settings

How to open the **List Management Settings** dialog:

1. Go to the **System** tab
2. Under **System settings**, double-click the **List Management Settings** tree node, as shown in the picture below:



3. When you double-click **List Management Settings** he dialog loads request the settings from the list management service and display them if successful. If loading fails, the error message is displayed to the user, and the dialog is closed.

List Management Settings dialog

In the dialog, you can find the following tabs:

- **Identities** - list of identities and their settings
- **Lists** - identity lists and their settings
- **Import/Export** - import/export functionality to restore/save list management data to CSV text format
- **Database Settings** - parameters related to the list management service database
- **Integration Settings** - integration enabling and integration settings

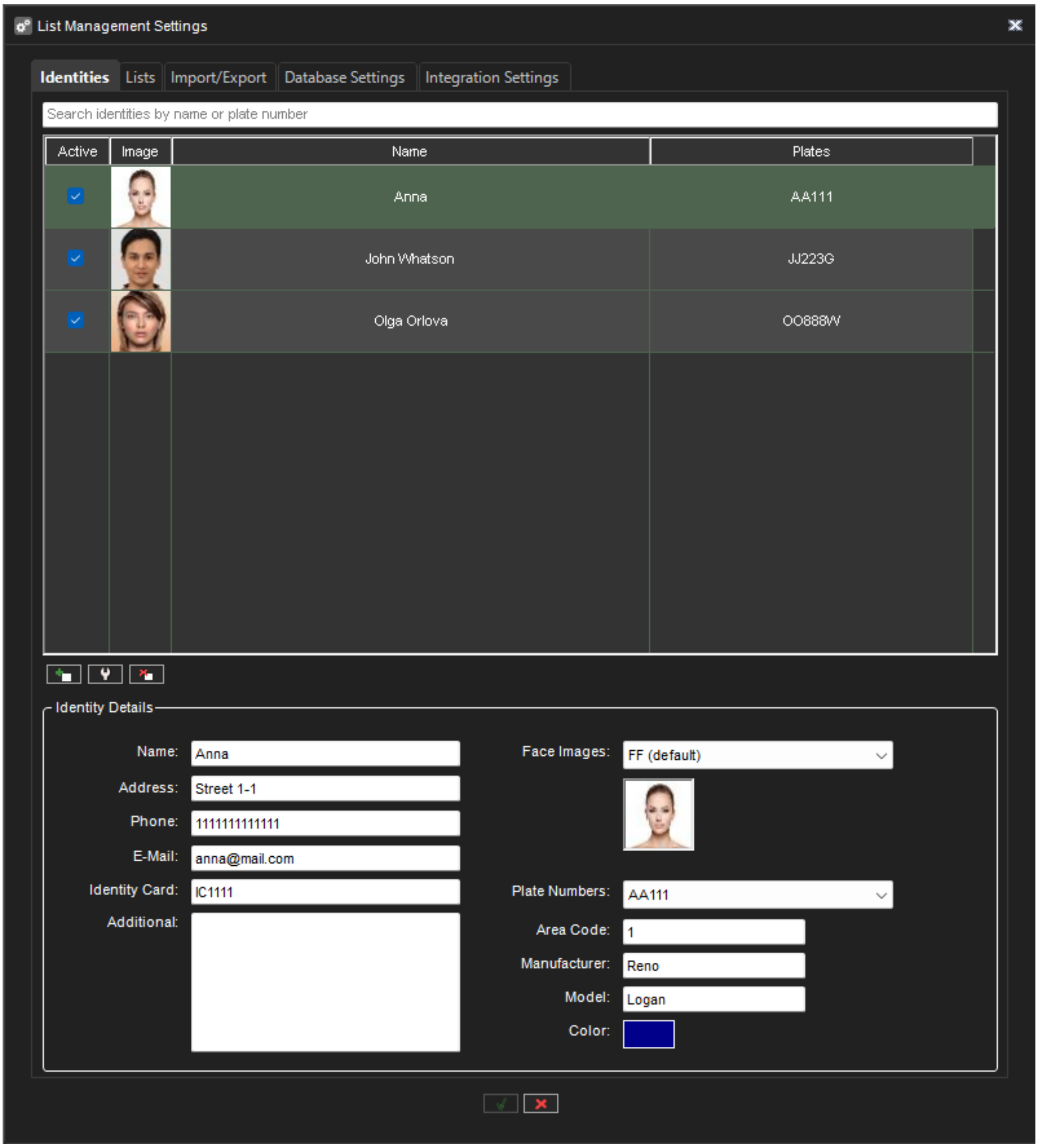
All changes you make in these dialog tabs can be saved by clicking the **OK** button.

If you do not need to keep the changes, you can close the dialog with the **Close** or the **Cancel** button.

Below you can find a detailed description of each tab.

Identities tab

In the “Identities” tab you can perform operations with identities:



Active	Image	Name	Plates
☑		Anna	AA111
☑		John Whatson	JJ223G
☑		Olga Orlova	OO888W

Name:	Anna	Face Images:	FF (default)
Address:	Street 1-1		
Phone:	111111111111		
E-Mail:	anna@mail.com		
Identity Card:	IC1111	Plate Numbers:	AA111
Additional:		Area Code:	1
		Manufacturer:	Reno
		Model:	Logan
		Color:	🟦

Figure 1 Identities tab

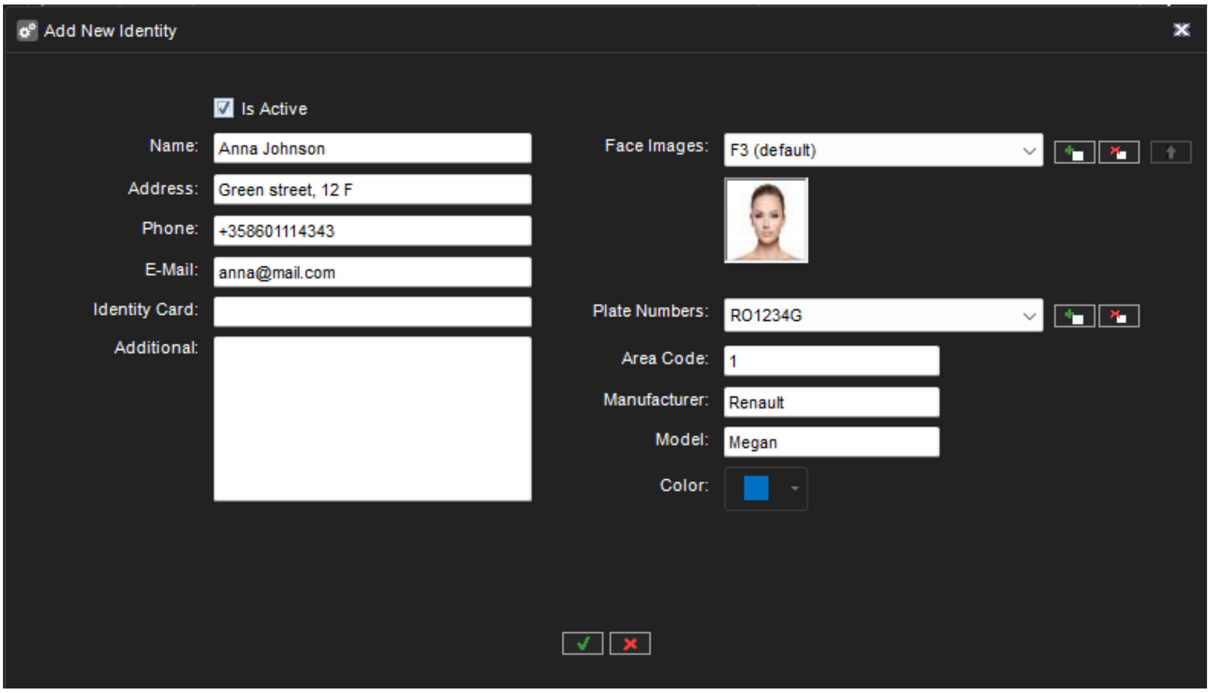
Identity selection is done using the left mouse button. If you must select multiple identities (multiple rows in the list), you can use the left mouse button + Ctrl/Shift keys. With multiple selections, you can set selected identities to the "active" or "not active" state by clicking the checkboxes in the “Active“ column.

Above the list of identities, you can find the **Search** field: when you type here, the list of identities is automatically filtered if the text is found in identity names or plates.

You can add and remove selected identities with the **Add** and **Remove** buttons below the identity list.

You can see detailed information about identity in the **Identity Details** area, but all these fields are read-only. To modify the selected identity, you can click the **Modify** button or double-click it with the mouse button.

When you add or modify identity, the following dialog is shown:



Add New Identity

☑ Is Active

Name: Anna Johnson

Address: Green street, 12 F

Phone: +358601114343

E-Mail: anna@mail.com

Identity Card:

Additional:

Face Images: F3 (default)

Plate Numbers: RO1234G

Area Code: 1

Manufacturer: Renault

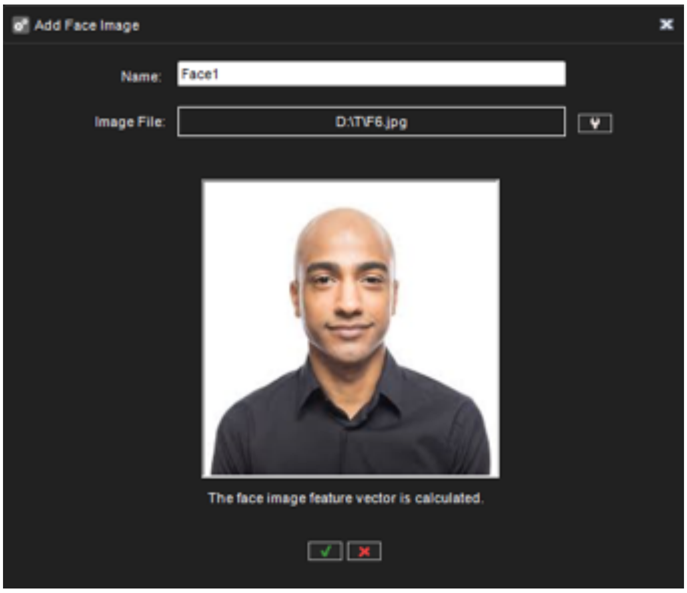
Model: Megan

Color: 🟦

Figure 2 Add/modify identity dialog

You can change any field data or add/remove identity face images or vehicles (license plates).

To add a face image, click the “Add a new face image” button, and the following dialog will open:



Name: Face1

Image File: D:\T\F6.jpg

The face image feature vector is calculated.

Figure 3 Add Face Image dialog

Several face images can be defined for an identity. All face images will be used when doing identity face matching, so using multiple face images for an identity, may increase the face detection confidence

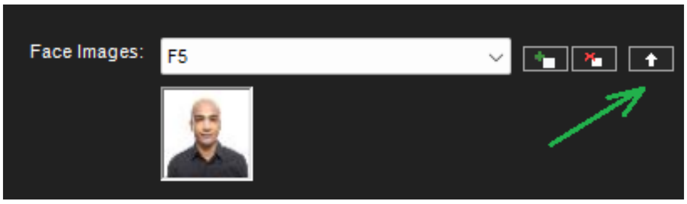
You can write a face image name and select a face image file here. After file selection, the image will be loaded, and the feature vector data of the image will be calculated.

To calculate the face feature vector, at least one face recognition service must be started and registered in VMS

To remove a face image, you need to select it in the combo box and click the **Remove Selected face image** button.

Set face image as default

One face image is the default, which is used as a thumbnail in all plugins and identity lists. To set the face image as the default, you need to select the face image in the combo box and click on the **Set selected face image as default** button:

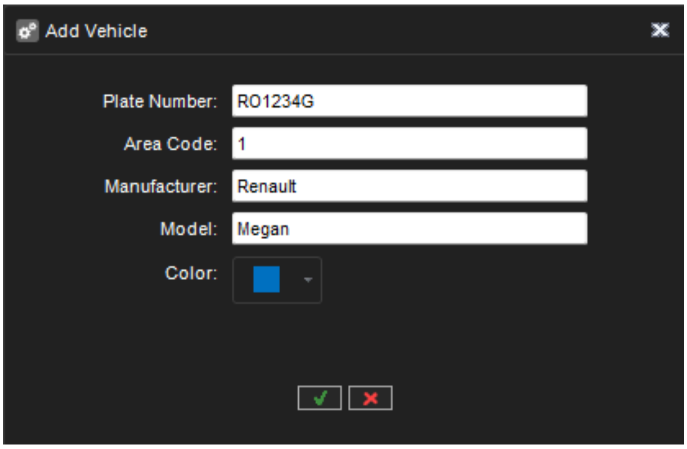


Face Images: F5

Figure 4 Set selected face image as default

Add or remove vehicles

You can add or remove vehicles. To add a vehicle, click the **Add a new vehicle** button, and the following dialog will open:



Add Vehicle

Plate Number: RO1234G

Area Code: 1

Manufacturer: Renault

Model: Megan

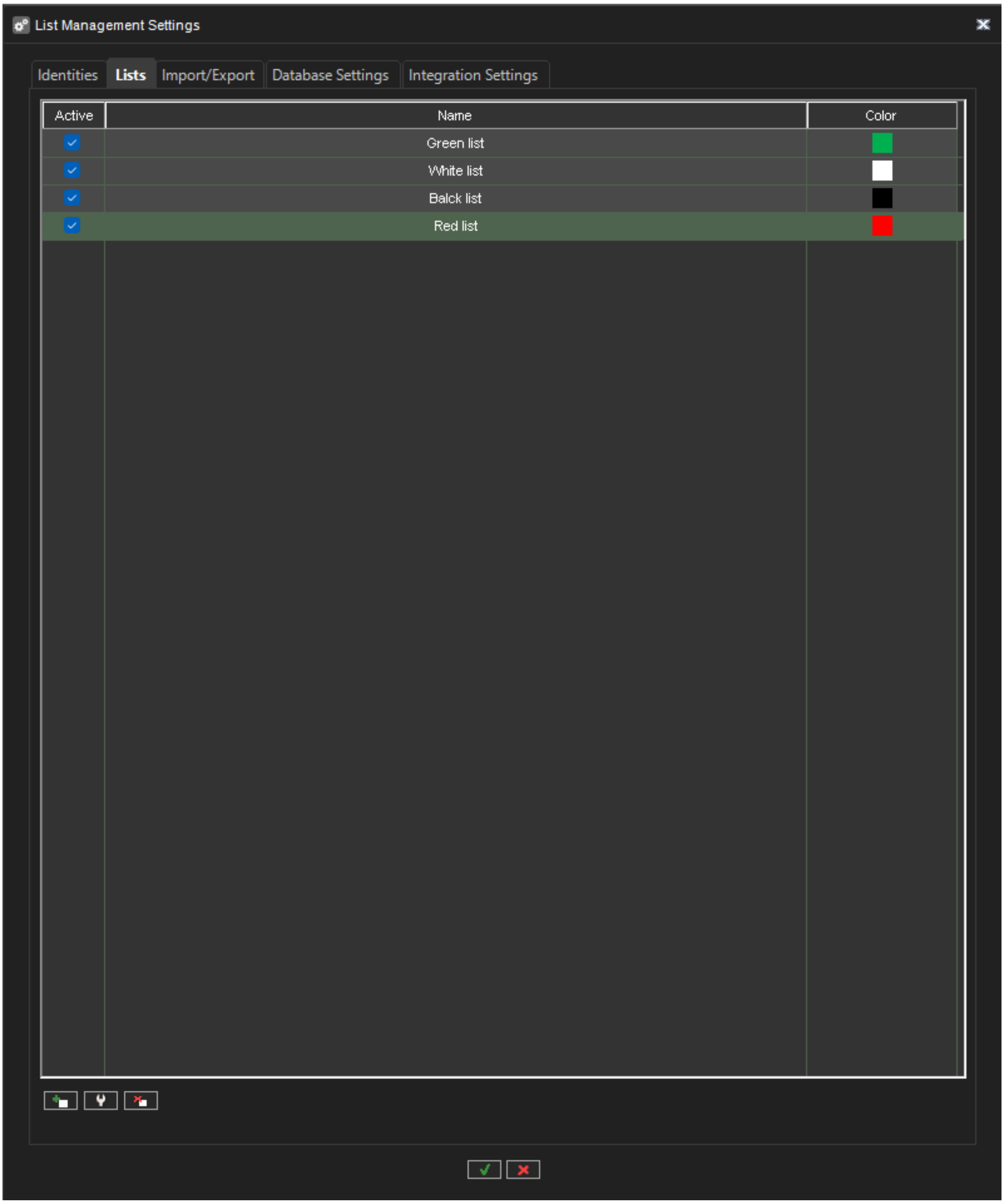
Color: 🟦

Figure 5 Add Vehicle dialog

In the **Add Vehicle** dialog, you can type the license plate number, area code, manufacturer, model, and vehicle color. To remove a vehicle, you need to select it in the combo box and click the **Remove selected vehicle** button.

Lists tab

In the **Lists** tab you can perform operations with identity lists:



List Management Settings

Active	Name	Color
☑	Green list	🟩
☑	White list	⬜
☑	Balck list	⬛
☑	Red list	🟥

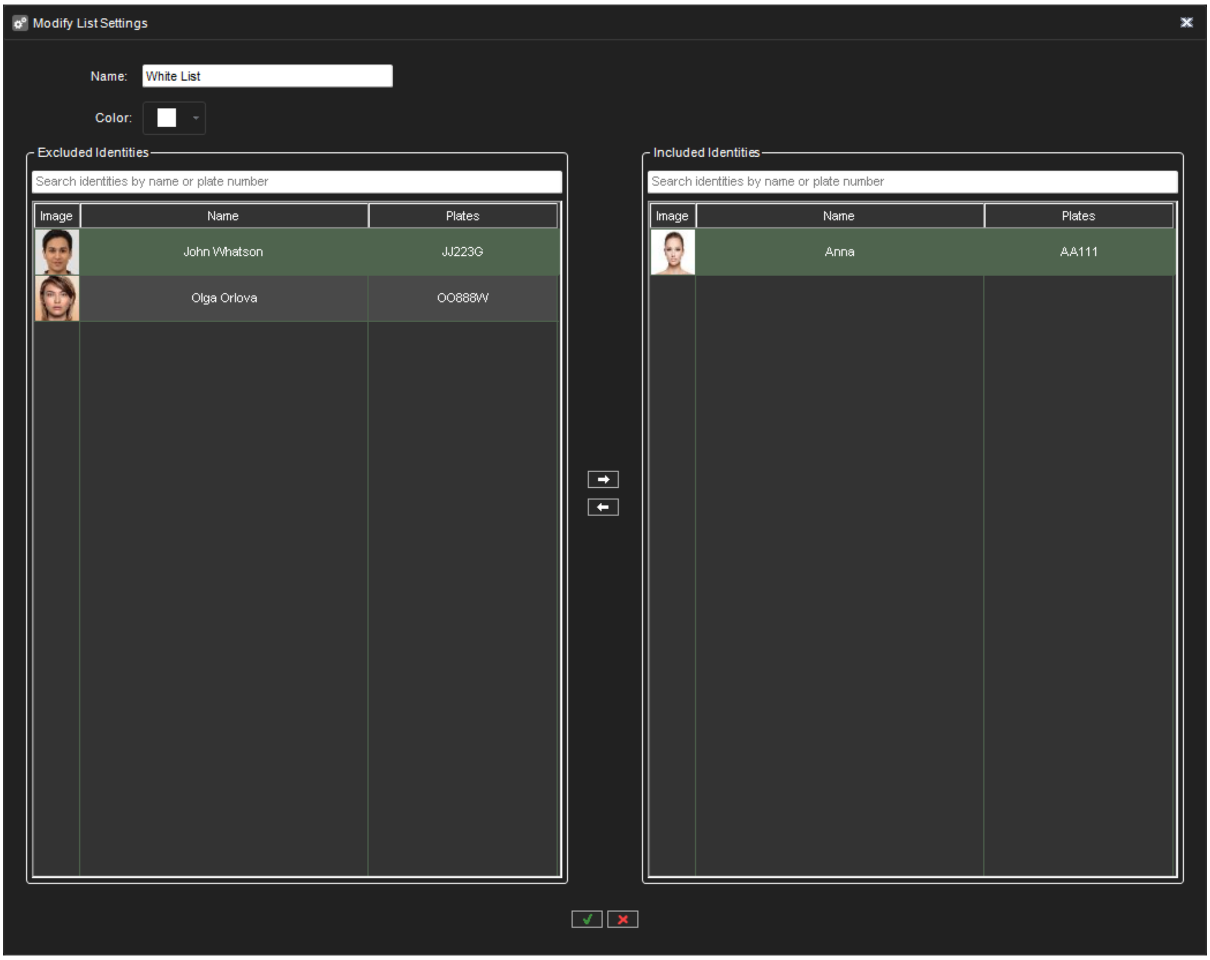
Figure 6 Lists tab

List selection is done using the left mouse button. If you need to select multiple lists (multiple rows), then you can use the left mouse button + Ctrl/Shift keys. With multiple selections, you can set selected lists to the **active** or **not active** state by clicking the checkboxes in the **Active** column.

You can add and remove selected lists with the **Add** and **Remove** buttons below the lists.

To modify the selected identity list, you can click the **Modify** button or double-click it with the mouse button.

When you add or modify the identity list, the following dialog is shown:



Modify List Settings

Name: White List

Color: ⬜

Excluded Identities

Search identities by name or plate number

Image	Name	Plates
	John Whatson	JJ223G
	Olga Orlova	OO888W

Included Identities

Search identities by name or plate number

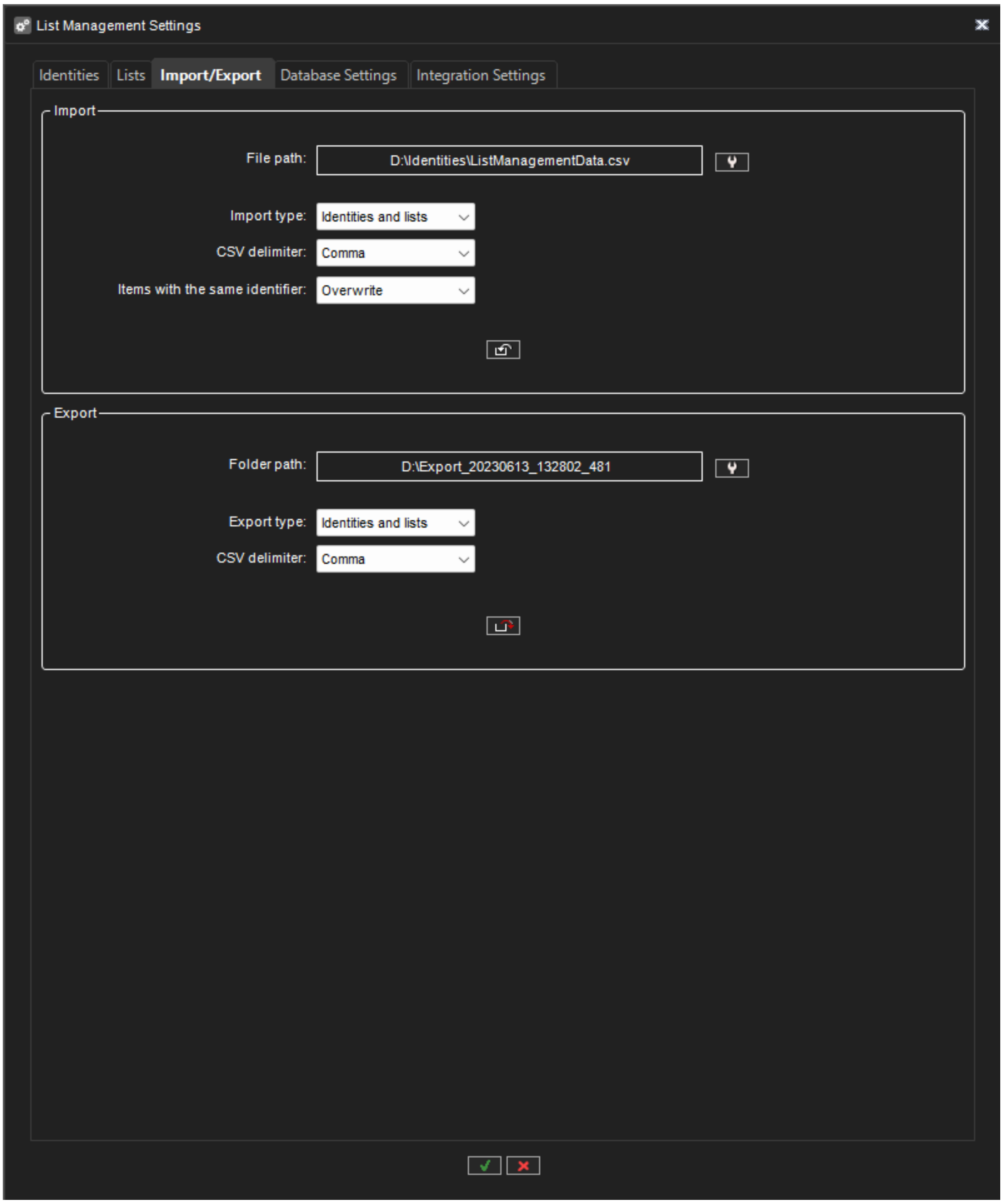
Image	Name	Plates
	Anna	AA111

Figure 7 Add/Modify List Settings dialog

You can move identities to the list or remove them from the list, define the name of the list, and color.

Import/Export tab

In the "Import/Export" tab you can import list management data from a CSV file or export list management data to a CSV file:



List Management Settings

Import

File path: D:\Identities\ListManagementData.csv

Import type: Identities and lists

CSV delimiter: Comma

Items with the same identifier: Overwrite

Export

Folder path: D:\Export_20230613_132802_481

Export type: Identities and lists

CSV delimiter: Comma

Figure 8 Import/Export tab

Import parameters

The following parameters must be set for the import process:

1. **File path** - path to the CSV file which contains list management data
2. **Import type** - “Identities only“ or “Identities and lists“
3. **CSV delimiter** - “Comma” or “Semicolon“
4. **Items with the same identifier** - “Skip“ them, “Overwrite“ or “Create new“ identifier for them

When the correct parameters are selected, the **Import data from file** button is active, and users can start the import process. During the process, users will see the progress and result of the import.

Export parameters

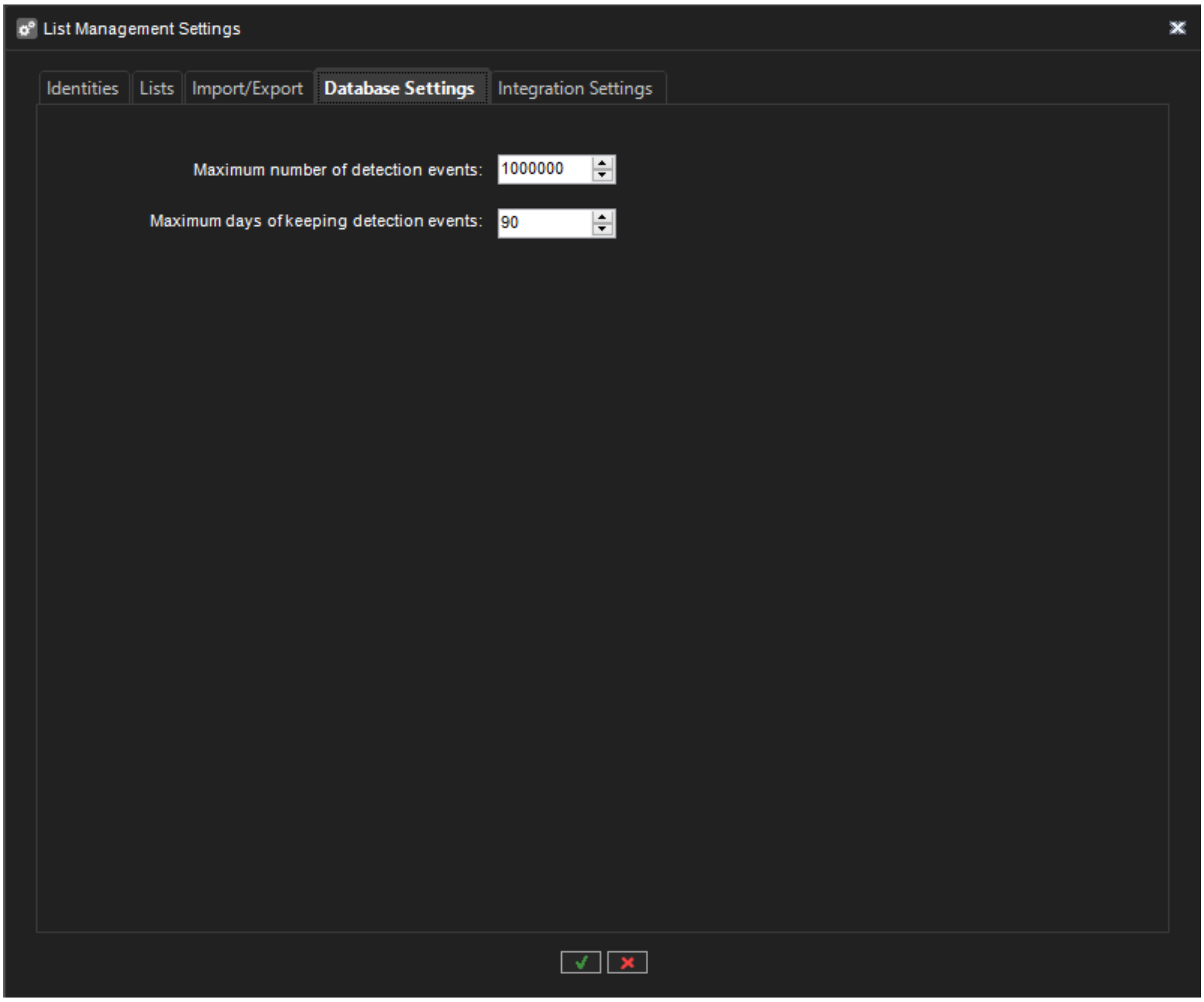
The following parameters must be set for the export process:

- **Folder path** - path to the folder where list management data will be exported and where the CSV file will be created
- **Export type** - “Identities only“ or “Identities and lists“
- **CSV delimiter** - “Comma” or “Semicolon“

When the correct parameters are selected, the “Export data to file“ button is active, and users can start the export process. During the process, users will see the progress and result of the export.

Database Settings tab

In the **Database Settings** tab, you can setup database settings for the list management service:



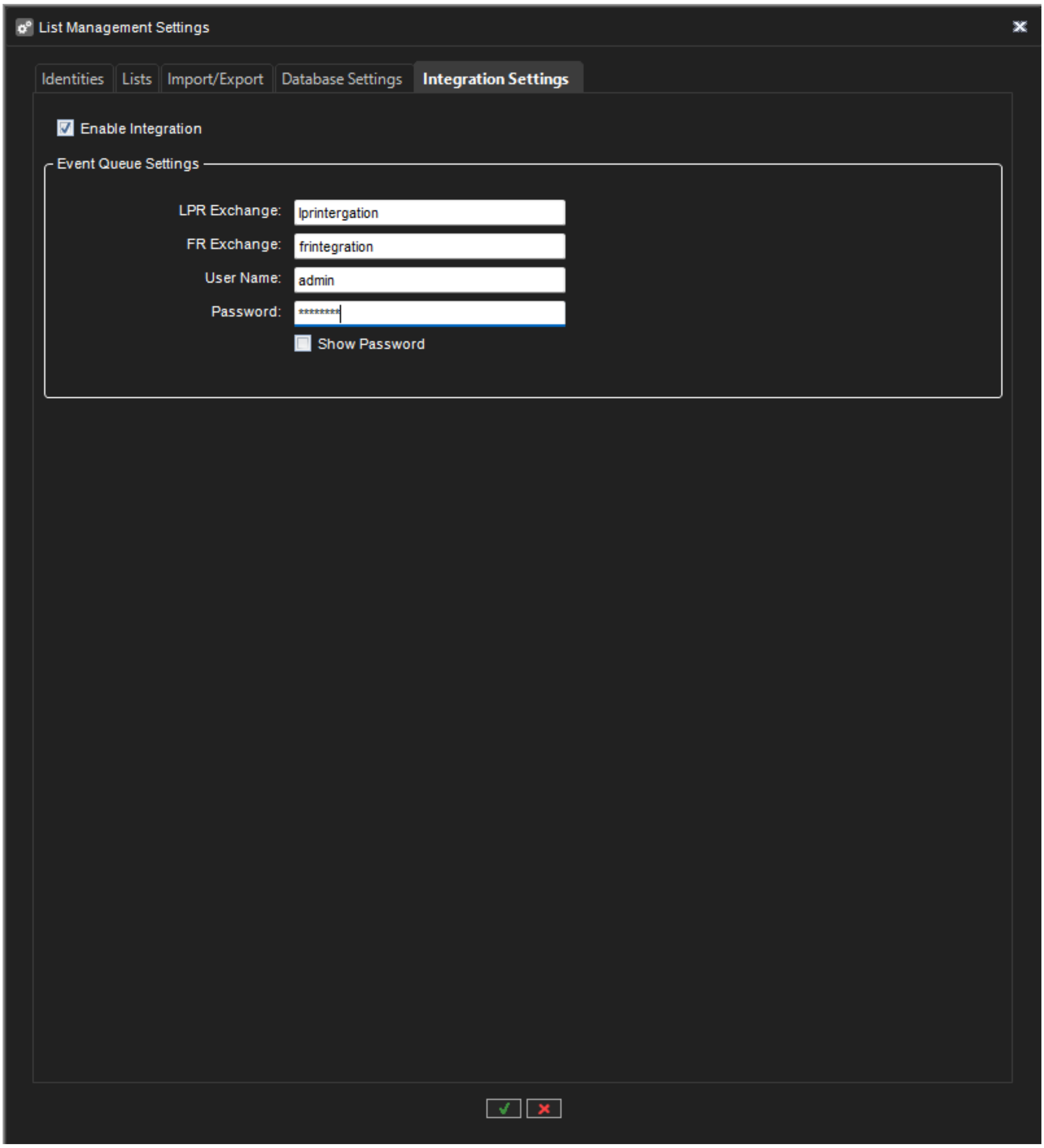
Maximum number of detection events: 1000000

Maximum days of keeping detection events: 90

Figure 9 Database Settings tab

Integration Settings tab

In the **Integration Settings** tab, you can setup integration settings for the list management service:



☑ Enable Integration

Event Queue Settings

LPR Exchange: lprintergation

FR Exchange: frintegration

User Name: admin

Password: ********

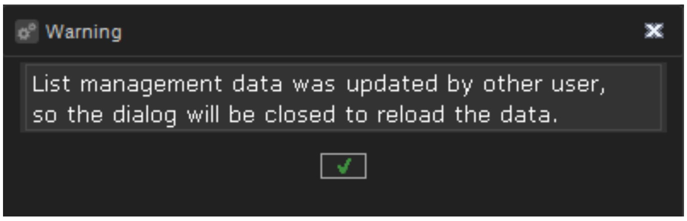
□ Show Password

Figure 10 Integration Settings tab

Here you can define settings for the event queue and enable/disable integration settings. The tab is not visible if the license does not enable list management integration.

List management data update notification

If list management data has been changed in another application, the System Manager will receive an event with updated information and display the following message:



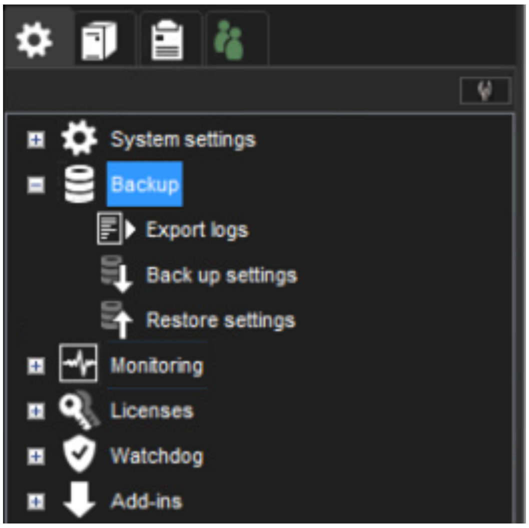
Warning

List management data was updated by other user, so the dialog will be closed to reload the data.

Figure 11 Data update warning

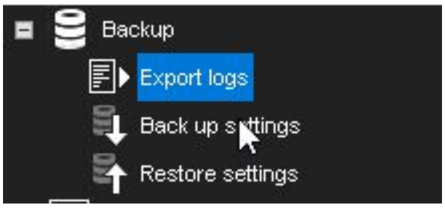
When you click the **OK** button of the message dialog, all settings dialogs will be closed to reload data from the list management service. All changes that were not saved will be lost.

Backup



Export logs

Export log files and send them to the system supplier should there be a problem with the system.



Log files are saved to a compressed (zipped) file that can be placed to a removable or non-removable device.

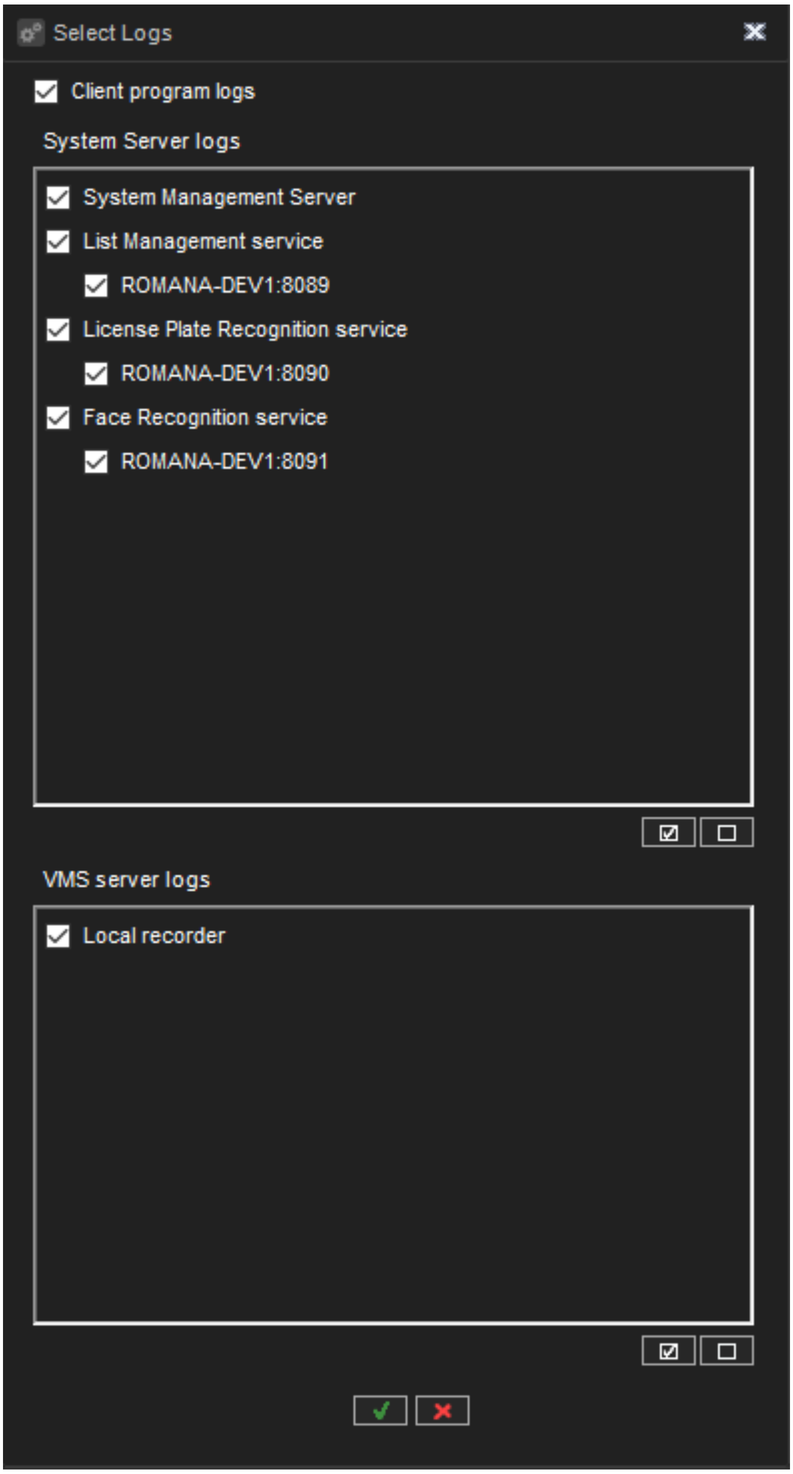
Export log files via System Manager

1. Open the System Manager application for export logs and choose the **Export logs** subitem in the **Backup** tree item on the **System** tab.
2. Select logs that can be exported in the

Select Logs window.

If there are problems with a server select logs on the **System Server logs** panel. In addition, select client program logs.

> The client logs are from the machine where you are accessing the system manager application.



Select Logs

☑ Client program logs

System Server logs

☑ System Management Server

☑ List Management service

☑ ROMANA-DEV1:8089

☑ License Plate Recognition service

☑ ROMANA-DEV1:8090

☑ Face Recognition service

☑ ROMANA-DEV1:8091

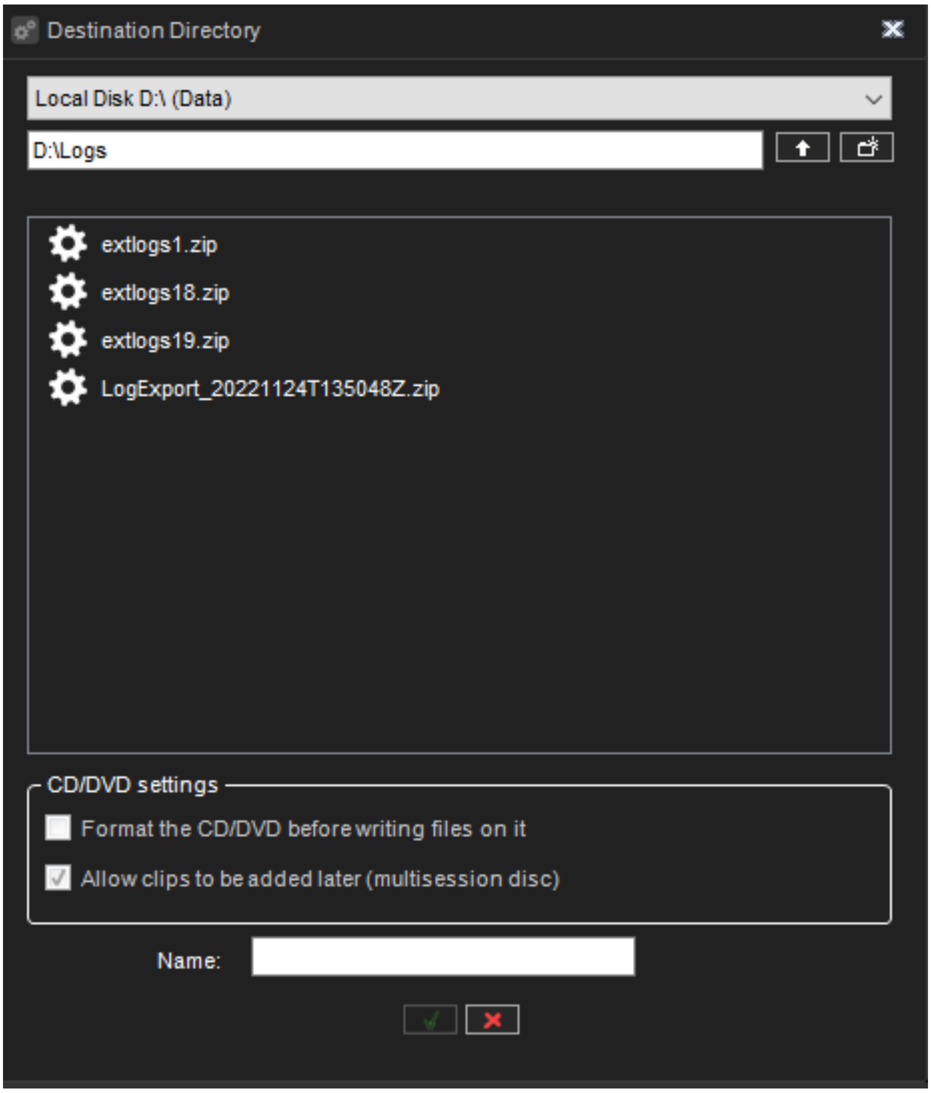
VMS server logs

☑ Local recorder

For fast selection, you can use the **Select All** and **Clear Selections** buttons placed under the **System Server logs** and **VMS server logs** panels. Select or clear all selections for specific service groups (e.g. **License Plate Recognition service**) that contain specific services by clicking on the services group checkbox.

3. Click **OK**.

4. Select the storage device and the folder where you want to save the log files in the **Destination Directory** window.



Destination Directory

Local Disk D:\ (Data)

D:\Logs

extlogs1.zip
extlogs18.zip
extlogs19.zip
LogExport_20221124T135048Z.zip

CD/DVD settings

□ Format the CD/DVD before writing files on it

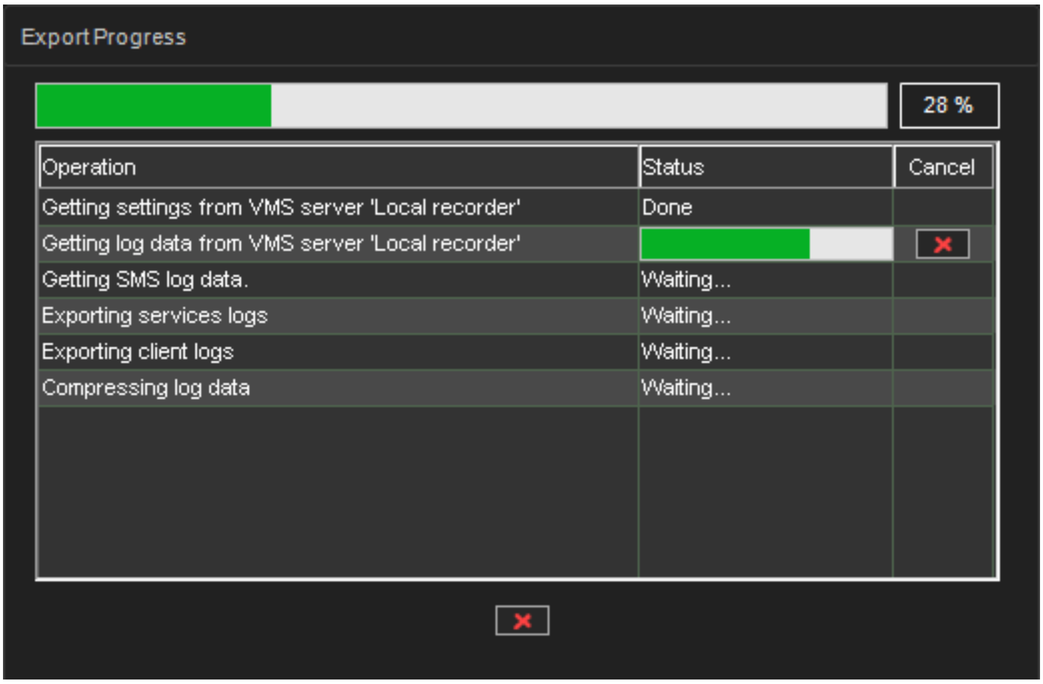
☑ Allow clips to be added later (multisession disc)

Name:

To create a new folder, click the **New folder** button.

Type a name for the ZIP file in the **Name** fields and click **OK**

You can see the progress of exporting in the **Export Progress** window. Operations are executed in order from top to bottom.



Export Progress

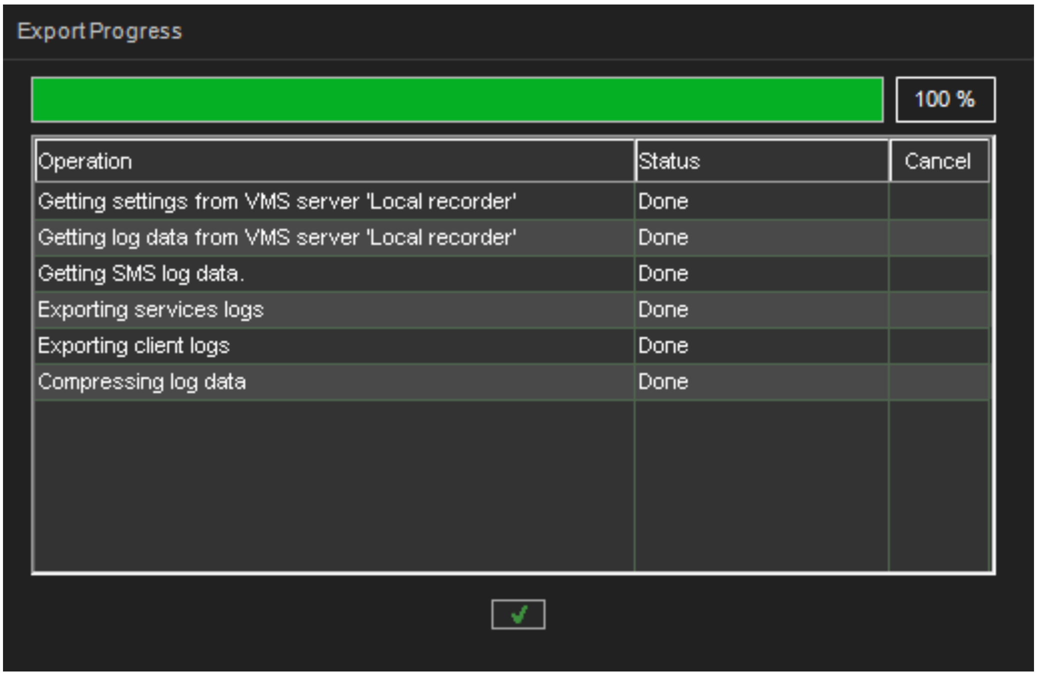
28 %

Operation	Status	Cancel
Getting settings from VMS server 'Local recorder'	Done	
Getting log data from VMS server 'Local recorder'		✕
Getting SMS log data.	Waiting...	
Exporting services logs	Waiting...	
Exporting client logs	Waiting...	
Compressing log data	Waiting...	

It is seems like the operation is stuck it can be cancelled.

Cancel all export by clicking on the **Cancel** button at the bottom of the window.

5. Click **OK** to close the window once the export is completed.



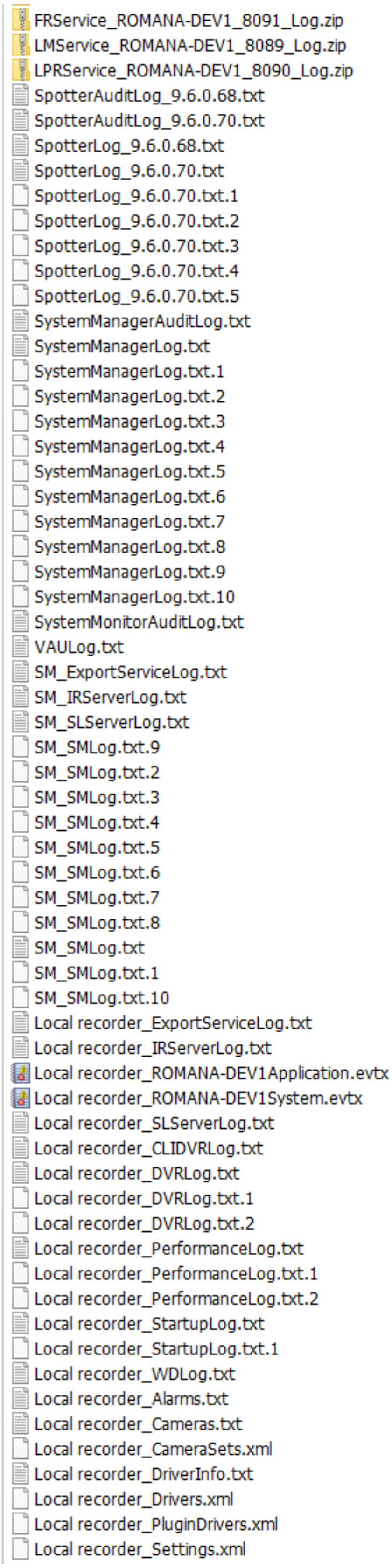
Export Progress

100 %

Operation	Status	Cancel
Getting settings from VMS server 'Local recorder'	Done	
Getting log data from VMS server 'Local recorder'	Done	
Getting SMS log data.	Done	
Exporting services logs	Done	
Exporting client logs	Done	
Compressing log data	Done	

6. The system exports the files to a ZIP file. Send the ZIP file to the system supplier. Services log files are stored in inner ZIP archives in the main ZIP file.

The typical content of logs ZIP archive is the following:



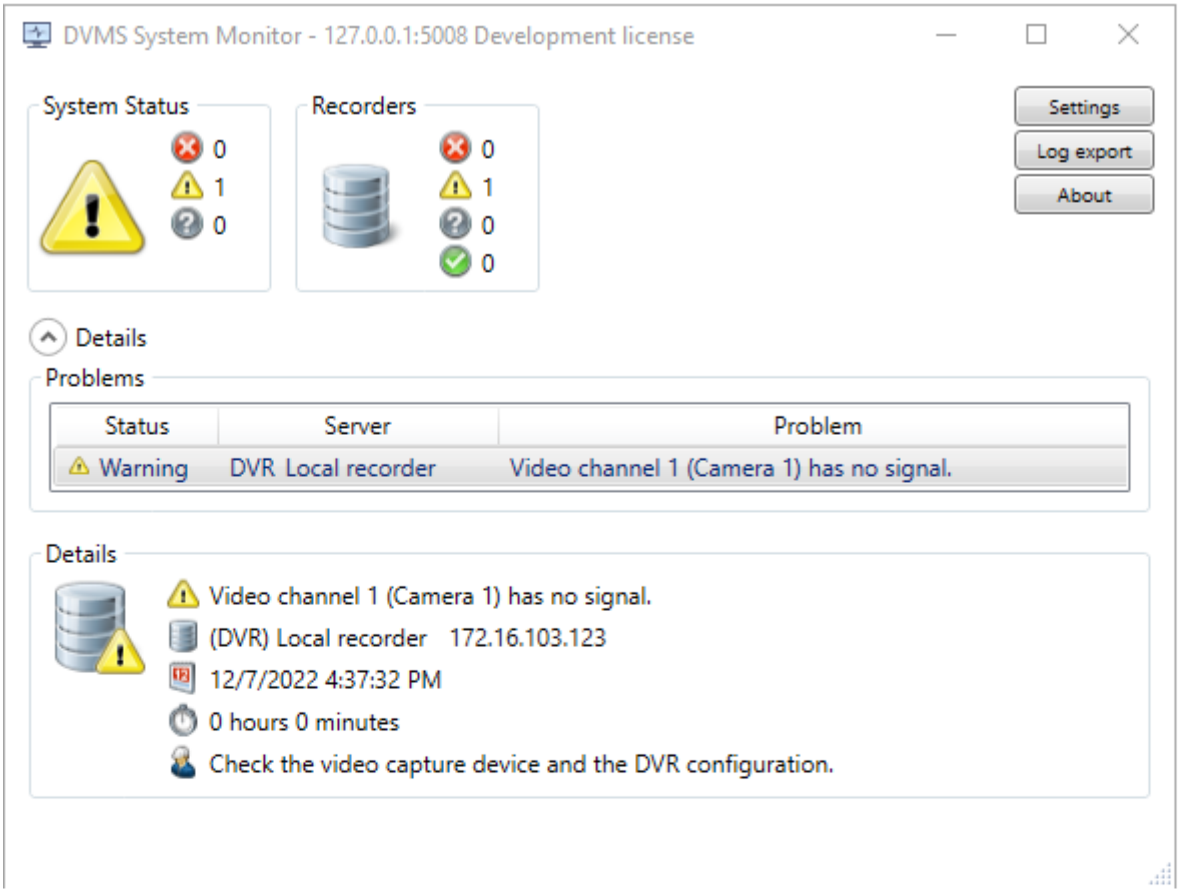
```
FRService_ROMANA-DEV1_8091_Log.zip
LMService_ROMANA-DEV1_8089_Log.zip
LPRService_ROMANA-DEV1_8090_Log.zip
SpotterAuditLog_9.6.0.68.txt
SpotterAuditLog_9.6.0.70.txt
SpotterLog_9.6.0.68.txt
SpotterLog_9.6.0.70.txt
SpotterLog_9.6.0.70.txt.1
SpotterLog_9.6.0.70.txt.2
SpotterLog_9.6.0.70.txt.3
SpotterLog_9.6.0.70.txt.4
SpotterLog_9.6.0.70.txt.5
SystemManagerAuditLog.txt
SystemManagerLog.txt
SystemManagerLog.txt.1
SystemManagerLog.txt.2
SystemManagerLog.txt.3
SystemManagerLog.txt.4
SystemManagerLog.txt.5
SystemManagerLog.txt.6
SystemManagerLog.txt.7
SystemManagerLog.txt.8
SystemManagerLog.txt.9
SystemManagerLog.txt.10
SystemMonitorAuditLog.txt
VAULog.txt
SM_ExportServiceLog.txt
SM_IRServerLog.txt
SM_SLServerLog.txt
SM_SMLog.txt.9
SM_SMLog.txt.2
SM_SMLog.txt.3
SM_SMLog.txt.4
SM_SMLog.txt.5
SM_SMLog.txt.6
SM_SMLog.txt.7
SM_SMLog.txt.8
SM_SMLog.txt
SM_SMLog.txt.1
SM_SMLog.txt.10
Local recorder_ExportServiceLog.txt
Local recorder_IRServerLog.txt
Local recorder_ROMANA-DEV1Application.evtx
Local recorder_ROMANA-DEV1System.evtx
Local recorder_SLServerLog.txt
Local recorder_CLIDVRLog.txt
Local recorder_DVRLog.txt
Local recorder_DVRLog.txt.1
Local recorder_DVRLog.txt.2
Local recorder_PerformanceLog.txt
Local recorder_PerformanceLog.txt.1
Local recorder_PerformanceLog.txt.2
Local recorder_StartupLog.txt
Local recorder_StartupLog.txt.1
Local recorder_WDLog.txt
Local recorder_Alarms.txt
Local recorder_Cameras.txt
Local recorder_CameraSets.xml
Local recorder_DriverInfo.txt
Local recorder_Drivers.xml
Local recorder_PluginDrivers.xml
Local recorder_Settings.xml
```

Some service sub-archives can be missed if there are no connections to services.

Export log files via System Monitor

It is possible to collect system logs via the System Monitor application.

1. Open System Monitor and click the
Log export button:



DVMS System Monitor - 127.0.0.1:5008 Development license

Problems

Status	Server	Problem
⚠ Warning	DVR Local recorder	Video channel 1 (Camera 1) has no signal.

Details

⚠ Video channel 1 (Camera 1) has no signal.
(DVR) Local recorder 172.16.103.123
12/7/2022 4:37:32 PM
0 hours 0 minutes
Check the video capture device and the DVR configuration.

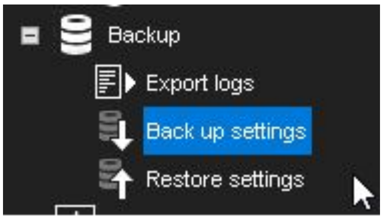
2. Choose the archive name and path for saving in the **Save as** dialog to save the export archive.

3. Click **Ok** to start collecting logs.

The System Monitor can collect **SM server** logs (also ones include **Incident Reporting** log, **Storage Locker** log, and **Export services** log), **DVRs** logs, clients' logs (**Spotter**, **System Manager**, etc.), and logs of all **List management**, **Face Recognition,** and **License Plate Recognition** services observed in the current system.

The typical content of logs ZIP archive is the same as for ZIP archive from System Manager. Some service sub-archives can be missed if there are no connections to services.

Back up settings



Backup system settings to be able to restore them if the hard disk that contains the settings fails.

You can back up system settings and server settings.

System settings contain data about the servers, profiles, and user accounts.

VMS Server settings contain data about the devices connected to the servers and their parameters.

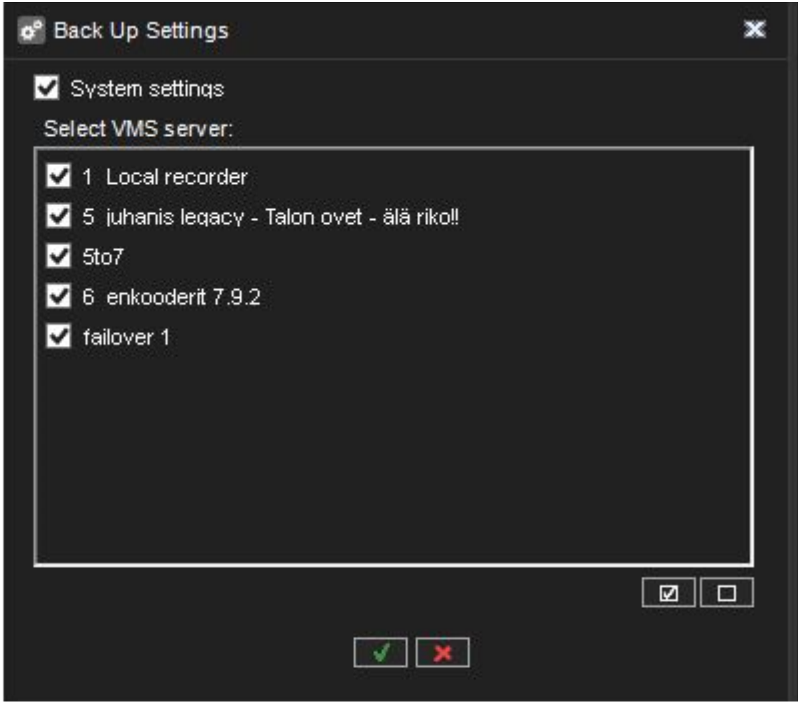
You can save the backup copy to a hard disk, network drive, CD/DVD, floppy disk, or another removable or non-removable device.

Backup files have the file extension “.vbk”.

To backup settings:

1. On the **System** tab, open **Backup settings**. The **Backup settings** dialogue box is shown.
2. Select the system and server-specific settings that you want to back up and click **OK**.
3. Select the storage device and the folder where you want to save the backup file. To create a new folder, click the **New folder** button.

4. Type a name for the file and a description and click **OK**. The description is optional. The system creates the backup file.



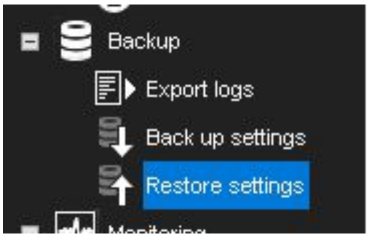
Back Up Settings

☑ System settings

Select VMS server:

☑ 1 Local recorder
☑ 5 juhanis legacy - Talon ovet - älä riko!!
☑ 5to7
☑ 6 enkooderit 7.9.2
☑ failover 1

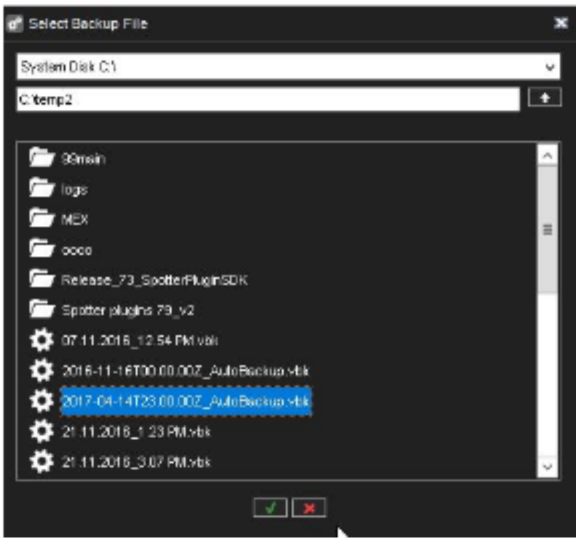
Restore settings



If you have created a backup file of the system and server settings, you can restore the settings if a problem occurs.

To restore settings:

1. On the **System** tab, open **Restore settings**. The Select backup file dialogue box is shown.



Select Backup File

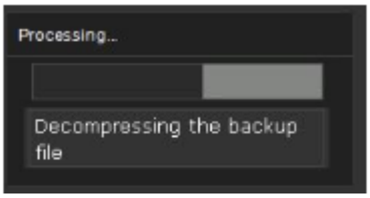
System Disk C:\

C:\temp2

99main
logs
MEX
oooo
Release_73_SpotterPluginSDK
Spotter plugins 79_v2
07.11.2016_12.54 PM.vbk
2016-11-16T00.00.00Z_AutoBackup.vbk
2017-04-14T23.00.00Z_AutoBackup.vbk
21.11.2016_1.23 PM.vbk
21.11.2016_3.07 PM.vbk

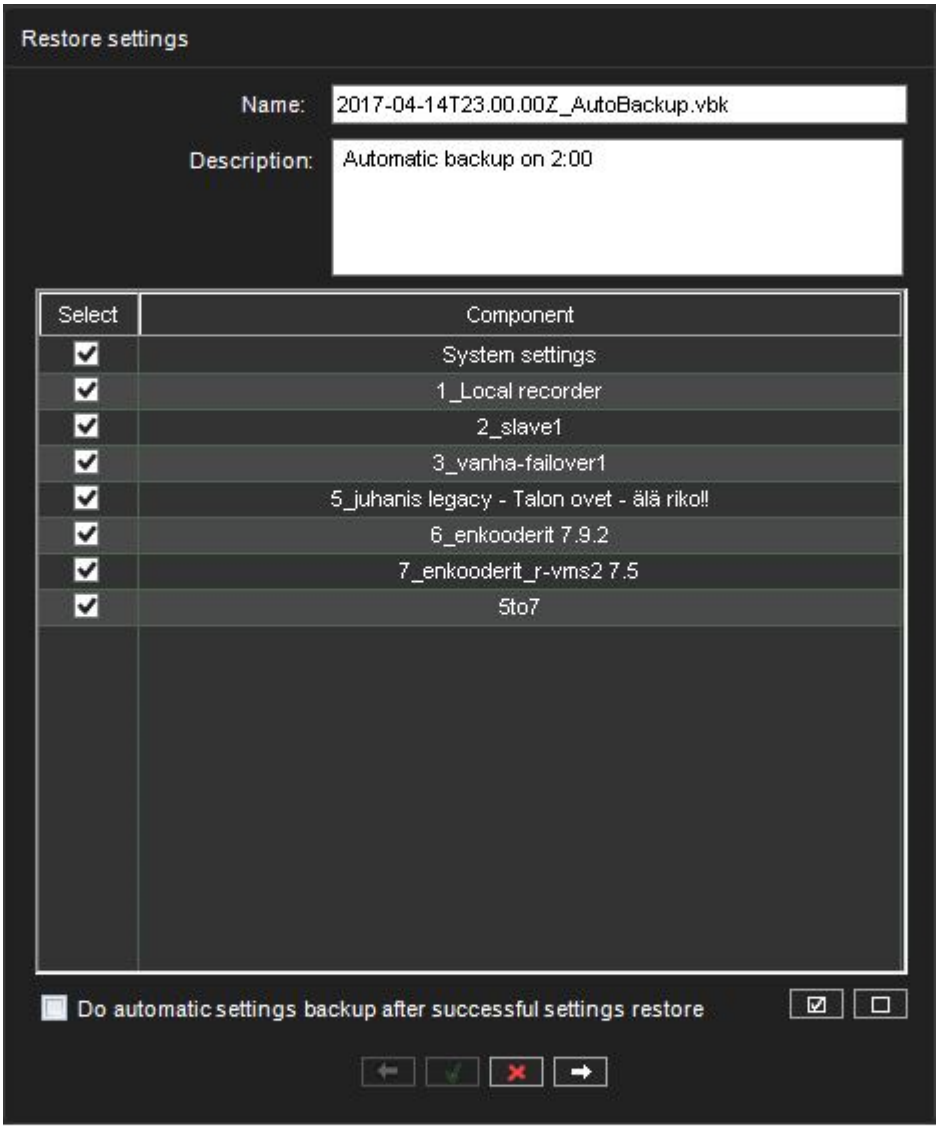
2. Find and select the backup file (.vbk) and click **OK**. The system decompresses the file and then shows the **Restore settings** dialogue box.

The dialogue box also shows a description of the settings.



Processing...

Decompressing the backup file



Restore settings

Name: 2017-04-14T23.00.00Z_AutoBackup.vbk

Description: Automatic backup on 2:00

Select	Component
☑	System settings
☑	1_Local recorder
☑	2_slave1
☑	3_vanha-failover1
☑	5_juhanis legacy - Talon ovet - älä riko!!
☑	6_enkooderit 7.9.2
☑	7_enkooderit_r-vms2 7.5
☑	5to7

□ Do automatic settings backup after successful settings restore

3. Select the system and server-specific settings that you want to restore and click **Start Restore**. The settings are restored.

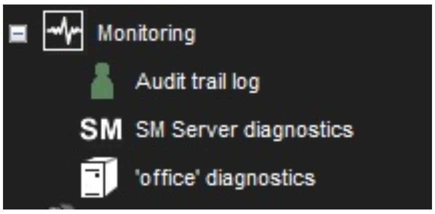
4. Click **OK** to accept the new settings or **Start the restore process again** to return to the **Restore settings** dialogue.

Do automatic settings backup after successful settings restore recommended, especially when restoring the system after failover has happened.

Monitoring

Audit trail log

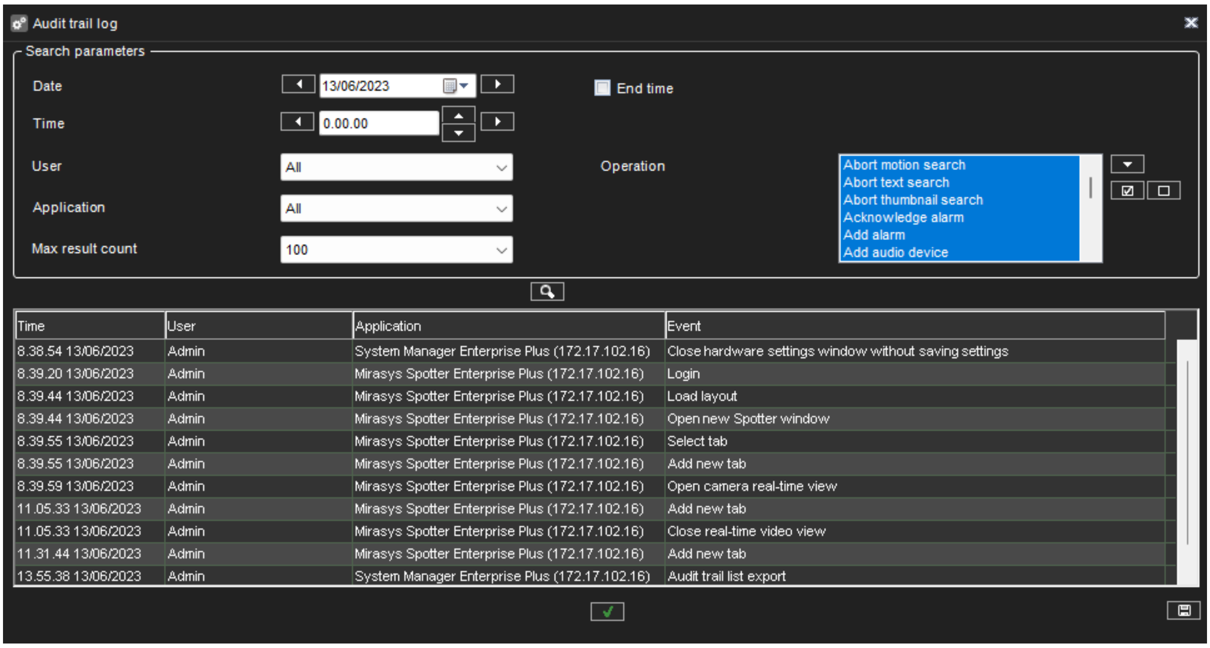
The Audit trail log can be used to search VMS system user activity information. It can be accessed in System Manager at the System tab tree under Monitoring.



Monitoring
Audit trail log
SM Server diagnostics
'office' diagnostics

Audit trail log

In the audit trail log dialog admin can search for audit trail events using several search parameters.



Audit trail log

Search parameters

Date: 13/06/2023
Time: 0.00.00
User: All
Application: All
Max result count: 100
□ End time
Operation: Abort motion search, Abort text search, Abort thumbnail search, Acknowledge alarm, Add alarm, Add audio device

Time	User	Application	Event
8.38.54 13/06/2023	Admin	System Manager Enterprise Plus (172.17.102.16)	Close hardware settings window without saving settings
8.39.20 13/06/2023	Admin	Mirasys Spotter Enterprise Plus (172.17.102.16)	Login
8.39.44 13/06/2023	Admin	Mirasys Spotter Enterprise Plus (172.17.102.16)	Load layout
8.39.44 13/06/2023	Admin	Mirasys Spotter Enterprise Plus (172.17.102.16)	Open new Spotter window
8.39.55 13/06/2023	Admin	Mirasys Spotter Enterprise Plus (172.17.102.16)	Select tab
8.39.55 13/06/2023	Admin	Mirasys Spotter Enterprise Plus (172.17.102.16)	Add new tab
8.39.59 13/06/2023	Admin	Mirasys Spotter Enterprise Plus (172.17.102.16)	Open camera real-time view
11.05.33 13/06/2023	Admin	Mirasys Spotter Enterprise Plus (172.17.102.16)	Add new tab
11.05.33 13/06/2023	Admin	Mirasys Spotter Enterprise Plus (172.17.102.16)	Close real-time video view
11.31.44 13/06/2023	Admin	Mirasys Spotter Enterprise Plus (172.17.102.16)	Add new tab
13.55.38 13/06/2023	Admin	System Manager Enterprise Plus (172.17.102.16)	Audit trail list export

The search button under the search parameters group starts the audit trail event search with selected parameters. Results are listed in the result list ordered by time. Found audit trail events can be sorted by other audit trail event information by clicking the list headers.

Search parameters

Following search parameters can be used for audit trail event searching.

1. **Date** - Select the date for the search to start. Buttons on the left and right decrease or increase the day of the date.
2. **Time** - Select the time of the date for the search to start. Buttons on the left and right decrease or increase the hour of the time. Buttons up and down increase or decreases minutes of the time by ten.
3. **End time check box** - If checked, it enables search end date and time selection similar way as for start time. If not checked, end time is not used as a search filter (= search until now)
4. **User** - User whose audit trail events will be searched. All = search without filtering users.
5. **Application** - Application to search. All = search without filtering applications.
6. **Max result count** - Maximum number for how many audit trail events will be searched starting from start time.
7. **Operation** - Operation to search: none, one, many, or all operations can select. If none or all is selected, then search without filtering operations. The following buttons can be used with operations:
    - Enlarge operation list view
    - Select all
    - Unselect all

Results list

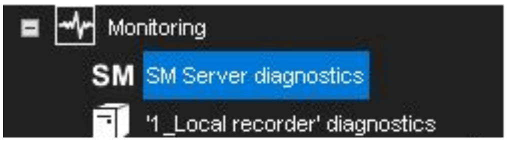
Found audit trail events are listed in the search result list. The list contains information about each audit trail event.

1. **Time** - Time of the user action.
2. **User** - Username who did the user action.
3. **Application** - Application where the user action was taken.
4. **Event** - Name of the user action.

Audit log export

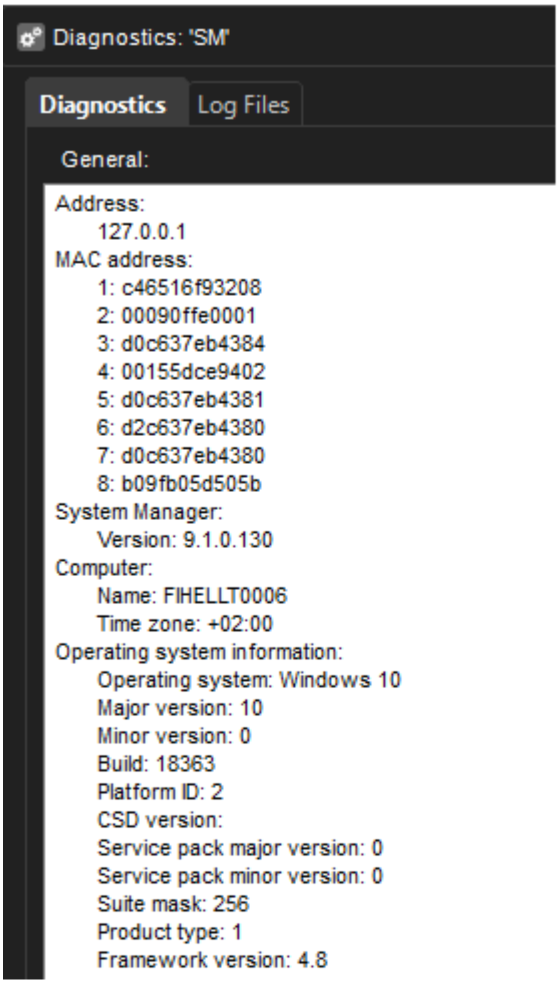
Listed audit trail events can be exported to a PDF file as an audit trail report by clicking the button under the audit trail events results list. The location and the name of the exported file and the comment for the report can be given on the save report dialog. The audit trail log report title is created of the export time and the user who exported the report. The report contains all the audit log entries with the same information that is listed in the audit trail event result list.

SM Server Diagnostics



SM Server Diagnostics shows information about the System Management Server that runs on the Master Server.

General



```
General:
Address:
      127.0.0.1
MAC address:
      1: c46516f93208
      2: 00090ffe0001
      3: d0c637eb4384
      4: 00155dce9402
      5: d0c637eb4381
      6: d2c637eb4380
      7: d0c637eb4380
      8: b09fb05d505b
System Manager:
      Version: 9.1.0.130
Computer:
      Name: FIHELLT0006
      Time zone: +02:00
Operating system information:
      Operating system: Windows 10
      Major version: 10
      Minor version: 0
      Build: 18363
      Platform ID: 2
      CSD version:
      Service pack major version: 0
      Service pack minor version: 0
      Suite mask: 256
      Product type: 1
      Framework version: 4.8
```

In SMServer Diagnostics, you can examine this information:

- SM Server version
- Computer name and time zone
- Operating system information
- Major version
- Minor version
- Build
- Platform ID
- CSD version
- Service pack major version

- Service pack minor version
- Suite mask
- Product type
- Framework version

Log Files

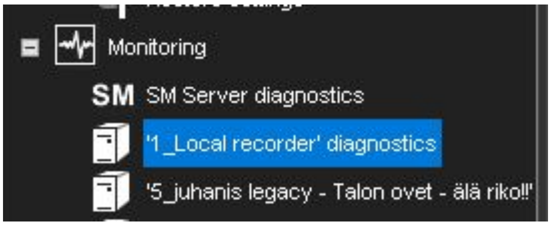
If there are problems with the system, you can access the system log files on the **Log Files** tab.

To examine a log file:

1. Select the file from the drop-down list.

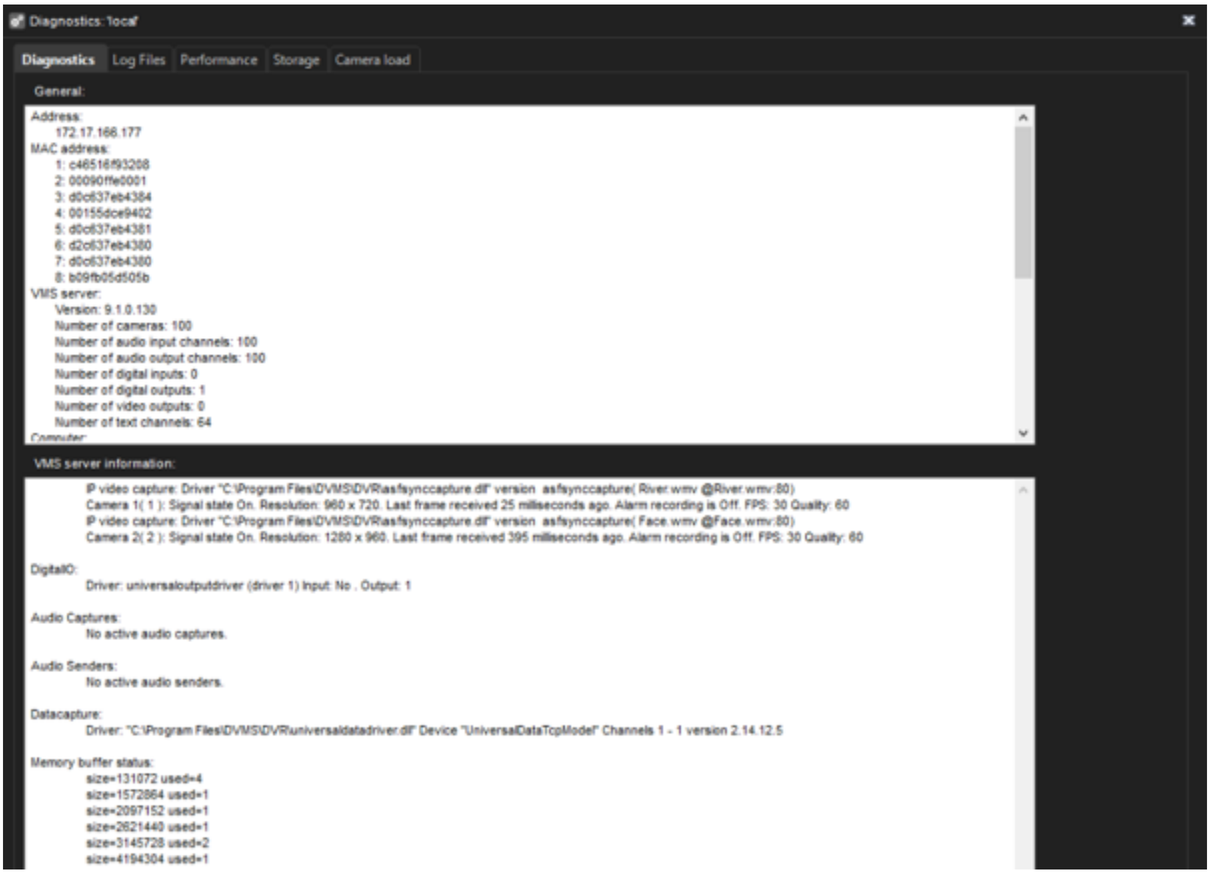
The contents are shown in the **Contents of the selected log file.**

Server Diagnostics


Monitoring
SM
SM Server diagnostics
'1_Local recorder' diagnostics
'5_juhanis legacy - Talon ovet - älä rikol!'

VMS Server diagnostics shows information about the server and the CPU and network usage.

Diagnostics



General:

```
Address:
    172.17.166.177
MAC address:
    1: c46516f93208
    2: 00090ffe0001
    3: d0c637eb4384
    4: 00155dce9402
    5: d0c637eb4381
    6: d2c637eb4380
    7: d0c637eb4380
    8: b09fb05d505b
VMS server:
    Version: 9.1.0.130
    Number of cameras: 100
    Number of audio input channels: 100
    Number of audio output channels: 100
    Number of digital inputs: 0
    Number of digital outputs: 1
    Number of video outputs: 0
    Number of text channels: 64
Computer:
```

VMS server information:

```
        IP video capture: Driver "C:\Program Files\DVMS\DVR\asfsynccapture.dll" version  asfsynccapture( River.wmv @River.wmv:80)
        Camera 1( 1 ): Signal state On. Resolution: 960 x 720. Last frame received 25 milliseconds ago. Alarm recording is Off. FPS: 30 Quality: 60
        IP video capture: Driver "C:\Program Files\DVMS\DVR\asfsynccapture.dll" version  asfsynccapture( Face.wmv @Face.wmv:80)
        Camera 2( 2 ): Signal state On. Resolution: 1280 x 960. Last frame received 395 milliseconds ago. Alarm recording is Off. FPS: 30 Quality: 60

DigitalIO:
        Driver: universaloutputdriver (driver 1) Input: No . Output: 1

Audio Captures:
        No active audio captures.

Audio Senders:
        No active audio senders.

Datacapture:
        Driver: "C:\Program Files\DVMS\DVR\universaldatadriver.dll" Device "UniversalDataTcpModel" Channels 1 - 1 version 2.14.12.5

Memory buffer status:
        size=131072 used=4
        size=1572864 used=1
        size=2097152 used=1
        size=2621440 used=1
        size=3145728 used=2
        size=4194304 used=1
```

The **Diagnostics** tab shows this information:

- Information about the server:
- Software version
- Model
- Number of cameras, audio channels, digital inputs, digital outputs, and video outputs
- The name of the computer and the time zone
- Operating system information
- Processor information
- Installed drivers, for example, capture drivers, video output drivers, digital output drivers, and PTZ drivers.

Log Files

The **Log files** tab shows a list of log files.

To see the contents of a log file:

- Select the file from the drop-down list. The contents are shown in the **Contents of the selected log file**.

Performance

On the **Performance** tab, you can monitor these:

- CPU usage.
- Usage of physical memory.
- Usage of virtual memory.
- Network traffic.
- Used disk space.

Storage

On the **Storage** tab, you can monitor disk and file properties. For example, you can examine free disk space or monitor saved data by the camera and audio channel.

GeneralTotal recording capacity. Shows the total storage capacity that is reserved for the recordings.

Used space. The quantity of space that the recordings have used.

Free space. Free space is available for recordings.

% used. The percentage of the disk's capacity that is used.

Average saving speed. Calculated by dividing the quantity of data saved since the server was last started by the uptime.

VMS Server uptime. Shows the time that the server has been operating since it was last started. The counter shows the difference between the current time and the start time in days, hours and minutes.

DisksTotal recording capacity. Shows the storage capacity that is reserved for the recordings on the selected disk.

Used space. Used recording space on the selected disk.

Free space. Free space is available for recordings on the selected disk.

% used. The percentage of space used of the total capacity reserved for the recordings.

Total recording cache. Shows the total capacity of the cache that is used for the temporary storage of data before it is permanently written on a disk.

Because of the cache, video and audio can be recorded immediately when the server is started. The cache is also used for pre-event recording.

The system automatically calculates how much cache space it must have and allocates space accordingly.

Used recording cache. Temporary space that is currently in use.

Free recording cache. Temporary space that is currently free.

CamerasOldest time. The date and time of the oldest image in the store.

Newest time. The date and time of the newest image in the store.

Total no. of images. The total number of images in the store.

Average image size. The average image size.

Used space. This value shows how much space the images and metadata files from this camera use.

% used. This value shows what percentage of space this camera has used of the total capacity reserved for the recordings.

Audio channels Oldest time. The date and time of the oldest audio sample in store.

Newest time. The date and time of the newest sample in store.

A total number of samples. The total number of audio samples in store.

Average sample size. The average audio sample size.

Used space. This value shows how much space the audio samples and metadata files from the audio channel use.

% used. This value shows what percentage of space the audio channel has used of the total capacity reserved for the recordings.

Text channels Oldest time. The date and time of the oldest text data sample in store.

Newest time. The date and time of the newest sample in store.

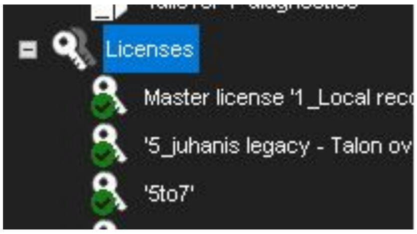
A total number of samples. The total number of text data samples in store.

Average sample size. The average text data sample size.

Used space. This value shows how much space the text data samples and metadata files from the text channel use.

% used. This value shows what percentage of space the text channel has used of the total capacity reserved for the recordings.

Licenses



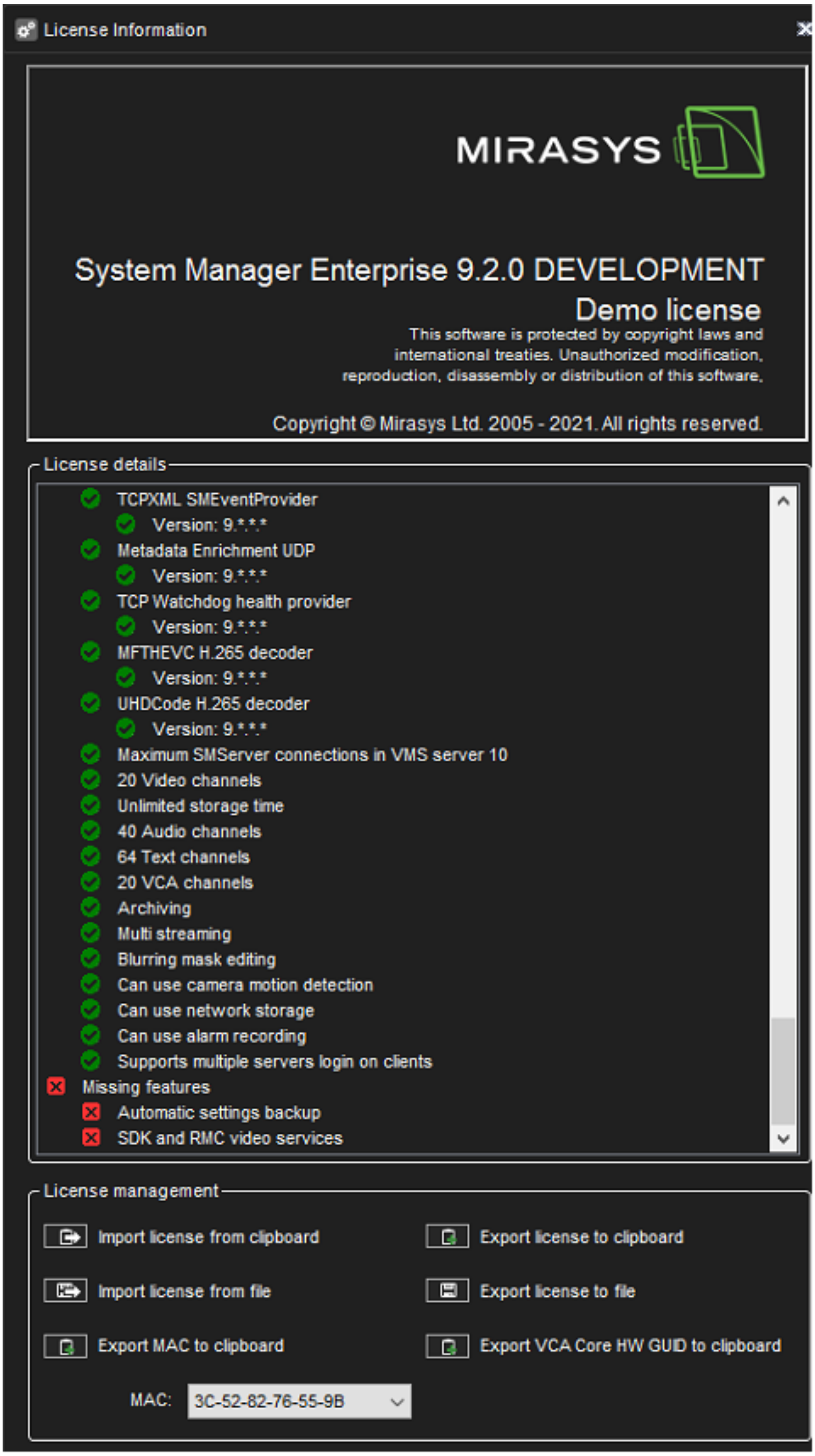
The server needs a valid license for full functionality.

Depending on the installation, you may need to upgrade the license information when adding new functionality or cameras to the system.

To get a license key, please contact your supplier and follow the license upgrade procedure as detailed by the supplier.

If you have any problems in upgrading the license, please contact *orders@mirasys.com*.

You can also add more camera channels and features such as VCA capabilities to a server by getting a new license key.



License Information

System Manager Enterprise 9.2.0 DEVELOPMENT

Demo license

This software is protected by copyright laws and international treaties. Unauthorized modification, reproduction, disassembly or distribution of this software,

Copyright © Mirasys Ltd. 2005 - 2021. All rights reserved.

License details

- ✓ TCPXML SMEventProvider
  - ✓ Version: 9.*.*.*
- ✓ Metadata Enrichment UDP
  - ✓ Version: 9.*.*.*
- ✓ TCP Watchdog health provider
  - ✓ Version: 9.*.*.*
- ✓ MFTHEVC H.265 decoder
  - ✓ Version: 9.*.*.*
- ✓ UHDCode H.265 decoder
  - ✓ Version: 9.*.*.*
- ✓ Maximum SMServer connections in VMS server 10
- ✓ 20 Video channels
- ✓ Unlimited storage time
- ✓ 40 Audio channels
- ✓ 64 Text channels
- ✓ 20 VCA channels
- ✓ Archiving
- ✓ Multi streaming
- ✓ Blurring mask editing
- ✓ Can use camera motion detection
- ✓ Can use network storage
- ✓ Can use alarm recording
- ✓ Supports multiple servers login on clients

☒ Missing features
- ☒ Automatic settings backup
- ☒ SDK and RMC video services

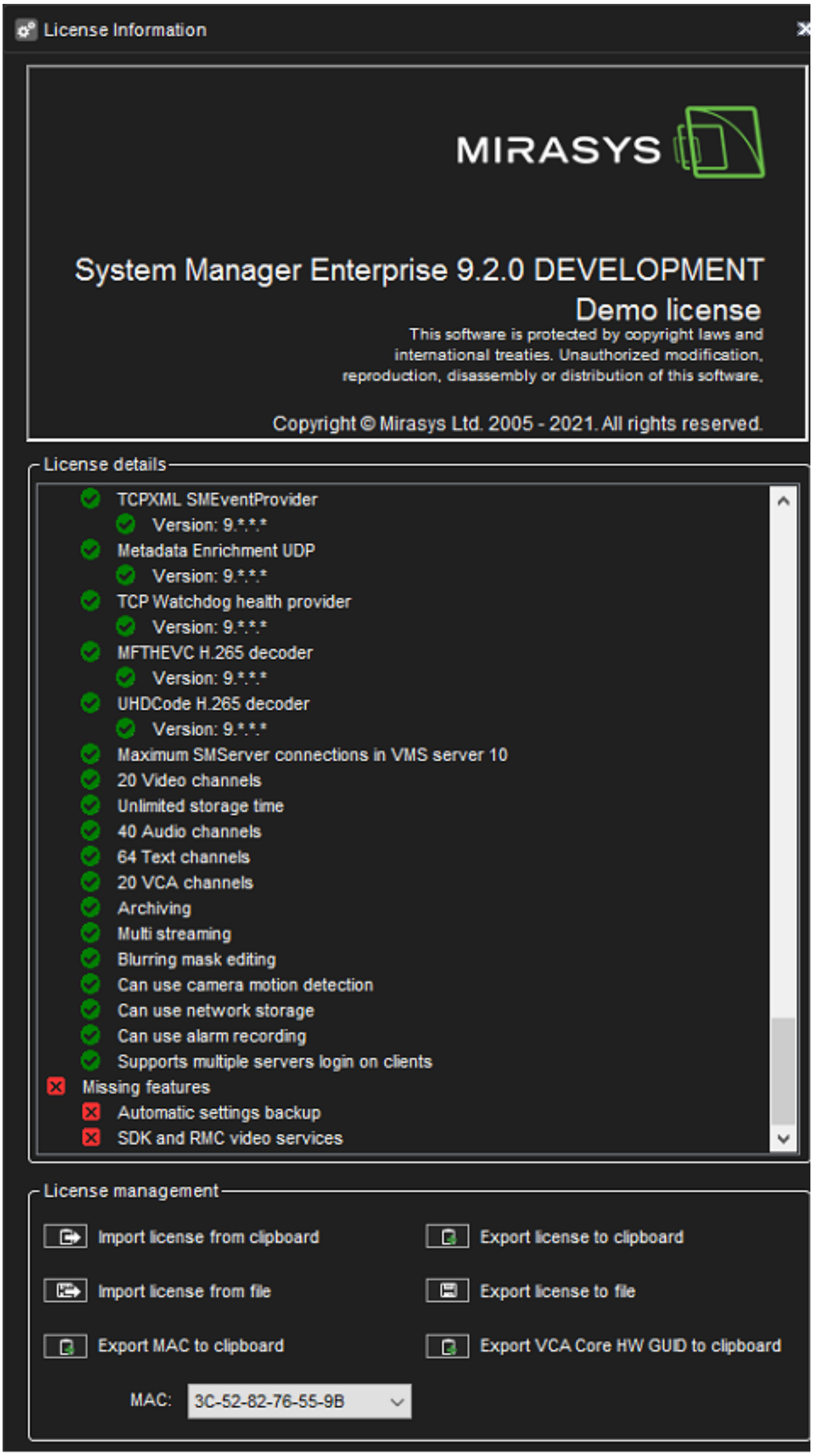
License management

Import license from clipboard
Export license to clipboard
Import license from file
Export license to file
Export MAC to clipboard
Export VCA Core HW GUID to clipboard

MAC: 3C-52-82-76-55-9B

License details

License details show all supported features of the license.



License Information

MIRASYS

System Manager Enterprise 9.2.0 DEVELOPMENT
Demo license

This software is protected by copyright laws and
international treaties. Unauthorized modification,
reproduction, disassembly or distribution of this software,

Copyright © Mirasys Ltd. 2005 - 2021. All rights reserved.

License details

```
    ✓ TCPXML SMEventProvider
        ✓ Version: 9.*.*.*
    ✓ Metadata Enrichment UDP
        ✓ Version: 9.*.*.*
    ✓ TCP Watchdog health provider
        ✓ Version: 9.*.*.*
    ✓ MFTHEVC H.265 decoder
        ✓ Version: 9.*.*.*
    ✓ UHDCode H.265 decoder
        ✓ Version: 9.*.*.*
    ✓ Maximum SMServer connections in VMS server 10
    ✓ 20 Video channels
    ✓ Unlimited storage time
    ✓ 40 Audio channels
    ✓ 64 Text channels
    ✓ 20 VCA channels
    ✓ Archiving
    ✓ Multi streaming
    ✓ Blurring mask editing
    ✓ Can use camera motion detection
    ✓ Can use network storage
    ✓ Can use alarm recording
    ✓ Supports multiple servers login on clients
☒ Missing features
    ☒ Automatic settings backup
    ☒ SDK and RMC video services
```

License management

Import license from clipboard
Export license to clipboard
Import license from file
Export license to file
Export MAC to clipboard
Export VCA Core HW GUID to clipboard

MAC: 3C-52-82-76-55-9B

License Management

To import a license key:

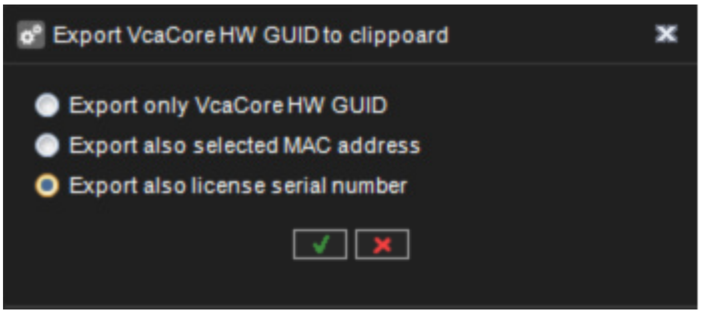
- Click **Import license from the file**.
- Browse to the license file location
- Click **OK**. The new license is updated immediately.

To export a license key:

- Click **Export license key to file** to create a text file for the license or **Export license key to the clipboard** to copy the key to the clipboard.
- If exporting the license to a file, set the destination folder and the name of the file.
- Click **OK**.

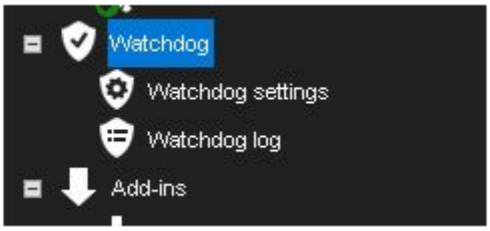
To export VCA Core HW GUID

- Click **Export VCA Core HW GUID to clipboard**
- Select **Export also license serial number**
- **Click Ok**


Export VcaCore HW GUID to clippoard

○ Export only VcaCore HW GUID
○ Export also selected MAC address
● Export also license serial number

Watchdog



The system has a software watchdog (system monitoring service) that monitors the system and performs specific actions if problems occur.

In the Watchdog tool, you can select the events for which the notification list is notified through e-mail and access watchdog logs, which contain the events that have occurred and the actions that have taken place.

Watchdog settings

In watchdog settings, you can select what events trigger a report to be sent to e-mail addresses specified in E-Mail Settings

You can select different events for each server.

Alternatively, you can select the same events for all servers by selecting **All VMS Servers** from the drop-down list.

In addition to e-mail notifications, notifications can be performed through digital outputs.

All event types are written to the watchdog logs, regardless of the e-mail settings.

To add or remove events on the notification list:

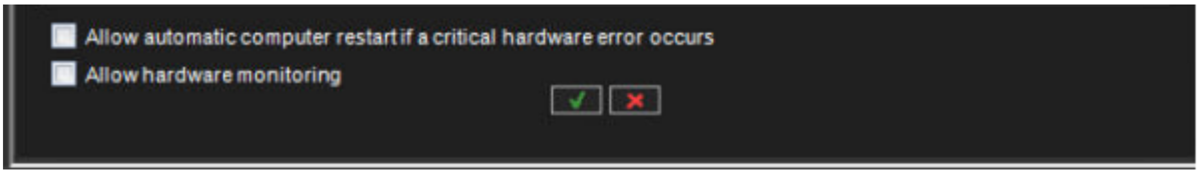
- On the **System** tab, select **Watchdog settings**.
- Mark the **Send mail** checkbox for each event type for which a notification e-mail should be sent.
- Click **OK**.

Automatic restart

Select the check box. **Allow automatic computer restart if a critical hardware error occurs** to restart the computer when serious hardware errors occur automatically.

The computer will not be restarted more than once a day.

Select **Allow hardware monitoring** if needed.



□ Allow automatic computer restart if a critical hardware error occurs

□ Allow hardware monitoring

Digital output notifications

In addition to e-mail notifications, notifications can be performed through digital outputs.

Notifications through digital output are created as server-specific; you need to select a specific server from the **VMS Server** drop-down list.

To set a digital output notification:

1. On the **System** tab, select **Watchdog settings**.
2. Select a server from the **VMS Server** drop-down list. As digital output signals are server-specific, you cannot select **All VMS Servers**.
3. Click on an event.
4. Select the digital output channel you want to use from the **In Use** drop-down menu.
5. If you want to send a pulse signal to the output channel, mark the **Pulse** checkbox and select the pulse length with the slider.
6. Click **OK**.

Watchdog log

By default, the system shows the watchdog logs from all servers.

However, you can select one or several servers from the list on the left.

You can sort the logs by clicking the column headings.

To update the list without closing the window, click the **Refresh** button.

Additional Watchdog Delivery Methods

The Watchdog functionality includes three new protocols: TCP, SMS (requires an external SMS module), and customizable e-mail form.

Each new protocol has its driver:

C:\Program Files\DVMS\DVR\WDEventProviders\

1. WDEventProviderSMS.xml
2. WDEventProviderSMTP.xml
3. WDEventProviderTCP.xml

At this moment, these files need to be edited manually. Each XML file contains the documentation regarding the configuration options.

The new configuration options include filtered and conditional warnings (i.e. “send warning X only once in every 60 minutes” or “send warning X only if condition Y is not met in two minutes”), and customizable warning message format.

After the files have been edited, Watchdog needs to be restarted for the changes to take effect.

***Note**: This feature is recommended only for advanced users. XML files are highly vulnerable to spelling errors and mistyped strings and keys.*

Even a tiny error can cause fatal errors. Mirasys takes no responsibility for XML errors caused by editing the files.

Watchdog event list

Id	Event	Description
0	SmServerDown	WDServer detected that SMServer process stopped
1	SmServerUp	WDServer detected that SMServer process started
2	DvrServerDown	WDServer detected that DVRService process stopped
3	DvrServerUp	WDServer detected that DVRServer process started

Id	Event	Description
4	NetworkDown	WDServer detected that network is down
5	NetworkUp	WDServer detected that network is up
6	DvrStatusOK	WDServer got ok status from recorder
7	DvrRefreshing	WDServer got settings refreshing status from recorder
8	DvrVideoCaptureLoadFailure	WDServer got video capture driver load error status from recorder
9	DvrAudioCaptureLoadFailure	WDServer got audio capture driver load error status from recorder
10	DvrDataCaptureLoadFailure	WDServer got text data driver load error status from recorder
11	DvrNoFileSystem	WDServer got no file system status from recorder
12	DvrDiskFailure	WDServer got disk failure status from recorder
13	VideoChannelOK	WDServer got video channel ok status from recorder
14	VideoChannelNoSignal	WDServer got video channel no signal status from recorder

Id	Event	Description
15	VideoChannelNotStarted	WDServer got video channel not started status from recorder
16	VideoChannelNoCapture	WDServer got video channel no capture status from recorder
17	AudioChannelOK	WDServer got audio channel ok status from recorder
18	AudioChannelNoSignal	WDServer got audio channel not started status from recorder
19	AudioChannelNotStarted	WDServer got audio channel no capture status from recorder
20	AudioChannelNoCapture	WDServer got audio channel not started status from recorder
21	DataChannelOK	WDServer got text data channel ok status from recorder
22	DataChannelNoSignal	WDServer got text data channel not started status from recorder
23	DataChannelNotStarted	WDServer got text data channel no capture status from recorder

Id	Event	Description
24	DataChannelNoCapture	WDServer got text data channel not started status from recorder
25	WDConnectionDown	Connection between WDServer and SMServer is down
26	WDConnectionUp	Connection between WDServer and SMServer is up
27	DvrSecurityFailure	WDServer got security failure status from recorder
28	DvrOtherInitFailure	WDServer got other initialization status from recorder
29	DvrArchiveFailed	WDServer got archive failed status from recorder
30	DvrMapNetworkDriveFailed	WDServer got map network drive failed status from recorder
31	DvrInsufficientDiskSpace	WDServer got insufficient disk space status from recorder
32	DvrNASDiskConnectionLostFailure	WDServer got NAS disk connection lost status from recorder

Id	Event	Description
33	DvrNASDiskInitializationFailure	WDServer got NAS disk initialization failed status from recorder
34	SMServerDBConnectionLost	SMServer has detected that database connection lost
35	SMServerDBConnectionRestored	SMServer has detected that database connection is restored
36	SMServerAuditTrailCacheFull	SMServer has detected that audit trail cache is full
37	DvrTemperatureLpcOk	NOT IN USE
38	DvrTemperatureLpcWarning	NOT IN USE
39	DvrTemperatureLpcFailure	NOT IN USE
40	DvrTemperatureCpuOk	NOT IN USE
41	DvrTemperatureCpuWarning	NOT IN USE
42	DvrTemperatureCpuFailure	NOT IN USE
43	DvrTemperatureHddOk	WDServer has detected that HDD temperature is ok
44	DvrTemperatureHddWarning	WDServer has detected that HDD temperature is in warning level

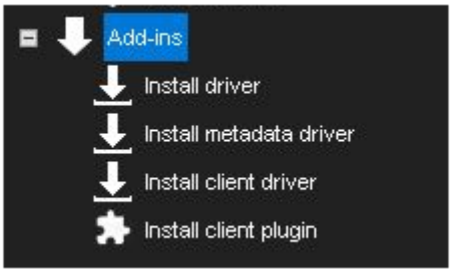
Id	Event	Description
45	DvrTemperatureHddFailure	WDServer has detected that HDD temperature is in failed level
46	DvrTemperatureDisplayAdapterOk	NOT IN USE
47	DvrTemperatureDisplayAdapterWarning	NOT IN USE
48	DvrTemperatureDisplayAdapterFailure	NOT IN USE
49	DvrTemperaturePsuOk	NOT IN USE
50	DvrTemperaturePsuWarning	NOT IN USE
51	DvrTemperaturePsuFailure	NOT IN USE
52	DvrTemperatureAcpiOk	NOT IN USE
53	DvrTemperatureAcpiWarning	NOT IN USE
54	DvrTemperatureAcpiFailure	NOT IN USE
55	DvrTemperatureRamOk	NOT IN USE
56	DvrTemperatureRamWarning	NOT IN USE
57	DvrTemperatureRamFailure	NOT IN USE
58	DvrMetadataDatabaseConnectionError	WDServer got metadata database connection error status from recorder

Id	Event	Description
59	GatewayUp	WDServer has detected that Gateway service is started
60	GatewayDown	WDServer has detected that Gateway service is stopped
61	DvrFatalRuntimeError	WDServer got fatal runtime error status from recorder
62	SMSServerUp	WDServer has detected that SMSServer service is started
63	SMSServerDown	WDServer has detected that SMSServer service is stopped
64	LicenseIsAboutToExpire	SMServer has detected that license is about to expire
65	LicenseHasExpired	SMServer has detected that license is expired
66	AutomaticBackupFailed	Automatic backup generation has failed in SMServer
67	DvrBrokenAtMaintenance	Recorder failure has been detected on maintenance mode and failover is ignored

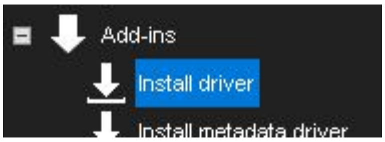
Id	Event	Description
68	DvrBrokenAndChangedWithFailoverDvr	Recorder failover has occurred
69	DvrBrokenWithoutPossibilityToChangeWithFailoverDvr	Recorder failure has been detected but there is no free failover servers
70	RPMServerUp	NOT IN USE
71	RPMServerDown	NOT IN USE
72	PublicWebApiServerUp	NOT IN USE
73	PublicWebApiServerDown	NOT IN USE
74	ExportServerUp	WDServer has detected that Export service has started
75	ExportServerDown	WDServer has detected that Export service has shutdown
76	StorageLockerServerUp	WDServer has detected that Storage Locker service has started
77	StorageLockerServerDown	WDServer has detected that Storage Locker service has shutdown
78	IncidentReportingServerUp	WDServer has detected that Incident Reporting service has started

Id	Event	Description
79	IncidentReportingServerDown	WDServer has detected that Incident Reporting service has shutdown
80	DvrFailbackDone	Recorder failback operation has been performed successfully on SMServer
81	DvrFailbackFailed	Recorder failback operation has failed on SMServer
82	DvrFailbackOnMaintenance	Recorder failback operation has been ignored because recorder is in maintenance mode

Add-ins



Installing External Driver Packages



To use IP cameras, digital I/O devices or text data in the VMS system, the driver for each device must be installed on the server.

The software includes all drivers and plugins that have been included in the previous versions of the software.

However, if necessary, new drivers and plugins can be installed manually.

To install a new driver, you need a device-specific driver installation package.

The driver installation package is a compressed (zipped) folder that contains the driver files.

When installing a driver installation package, the system compares the files in the installation package to the existing files on the servers.

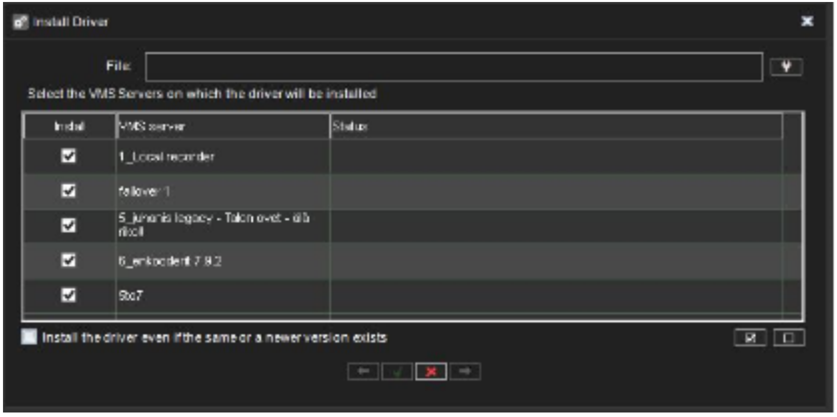
It usually installs the files only if they do not exist on the servers or if the files in the installation package are newer than the files on the servers.

However, you can force the system to install any driver version if necessary.

***Note**: If you want to update an already existing camera driver, remove the camera from the system before updating the driver.After removing the camera, install the driver file, after which you can reinstall the camera.After installing a new driver, you need to configure the devices that use the driver.*

To install a driver package:

1. On the **System** tab, under **Add-ins**, open **Install driver**.
2. Select the drive where the driver package is located, find and select the driver package (.zip file). The **Install Driver** dialogue box is shown.



File:

Select the VMS Servers on which the driver will be installed

Install	VMS server	Status
☑	1_Local recorder	
☑	failover 1	
☑	5_junaris legacy - Talon ovet - ää rikoll	
☑	6_enkoodert 7.8.2	
☑	Sto7	

□ Install the driver even if the same or a newer version exists

3. Select the servers on which you want to install the driver.

4. If you want to force the system to install the driver package version, select **Install the driver even if the same or a newer version exists.**

5. Click **Install**. The **Status** column shows the text **Installed** if the driver is successfully installed. If the driver is not installed, the column shows an error message.

6. Click **Close** to exit the dialogue box.

Notes*:*

- If you need to update drivers for hardware other than IP cameras, please contact the system supplier.
- A 32-bit system requires a 32-bit driver package, and a 64-bit system required a 64-bit driver package.

Installing Metadata Drivers

It is possible to update and install new metadata drivers using the **Install metadata drivers** –option in the **System** tab.

Installing Client Drivers

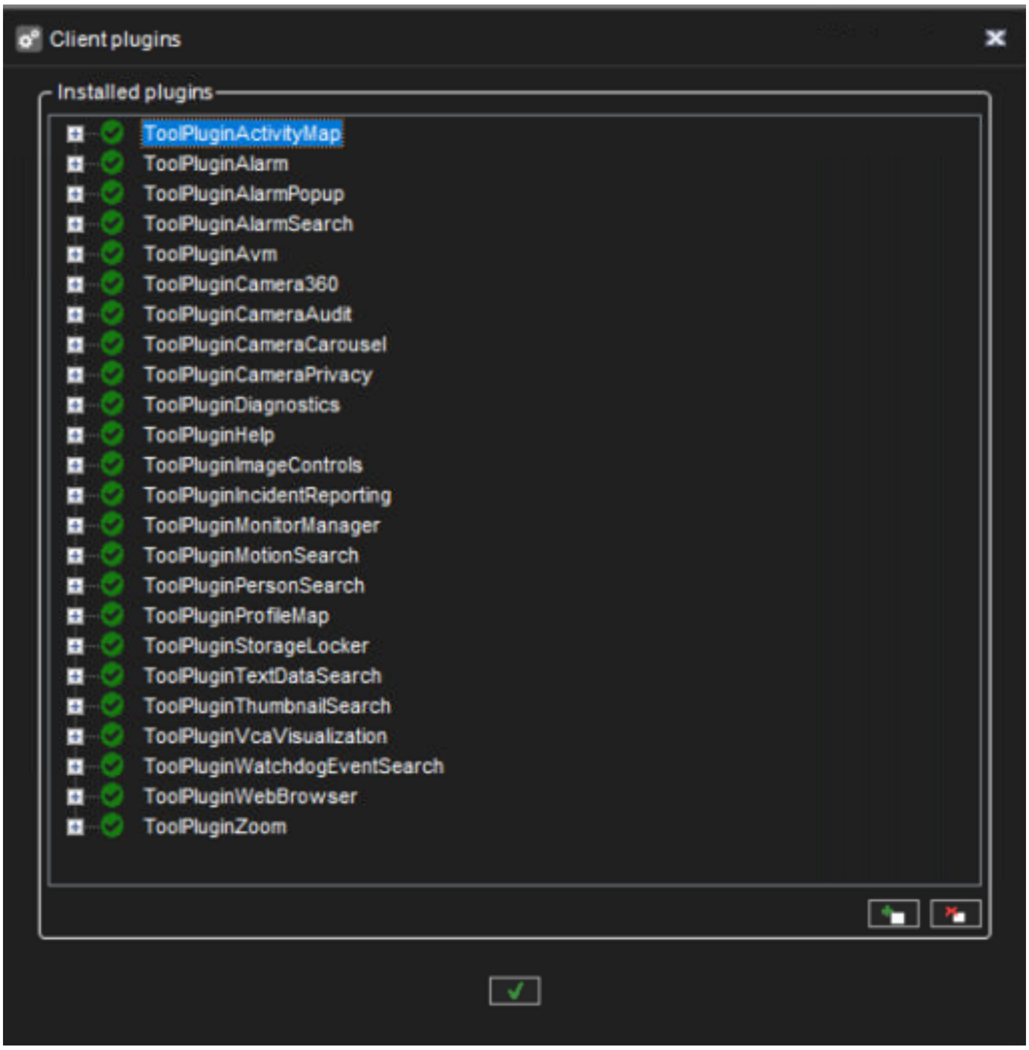
TruCast (direct streaming from camera to Spotter client) requires a different type of camera driver.

These are called (Managed) TruCast Client drivers.

The client camera drivers are installed similarly as spotter plugins and metadata drivers, using the **Install client driver** option in the system manager.

Install client plugin

Client plugins for user interfaces such as Spotter can be installed through System Manager.



Client plugins

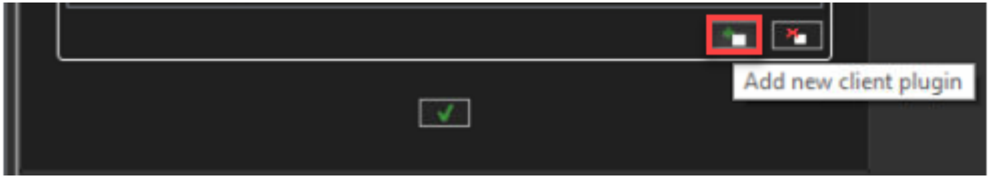
Installed plugins

- ToolPluginActivityMap
- ToolPluginAlarm
- ToolPluginAlarmPopup
- ToolPluginAlarmSearch
- ToolPluginAvm
- ToolPluginCamera360
- ToolPluginCameraAudit
- ToolPluginCameraCarousel
- ToolPluginCameraPrivacy
- ToolPluginDiagnostics
- ToolPluginHelp
- ToolPluginImageControls
- ToolPluginIncidentReporting
- ToolPluginMonitorManager
- ToolPluginMotionSearch
- ToolPluginPersonSearch
- ToolPluginProfileMap
- ToolPluginStorageLocker
- ToolPluginTextDataSearch
- ToolPluginThumbnailSearch
- ToolPluginVcaVisualization
- ToolPluginWatchdogEventSearch
- ToolPluginWebBrowser
- ToolPluginZoom

Plugin installation can be opened from the system tab under Add-ins.

To install a client plugin:

1. Open the **Install client plugin**.
2. Click **Add new client plugin**. Browse for the correct file and select it.

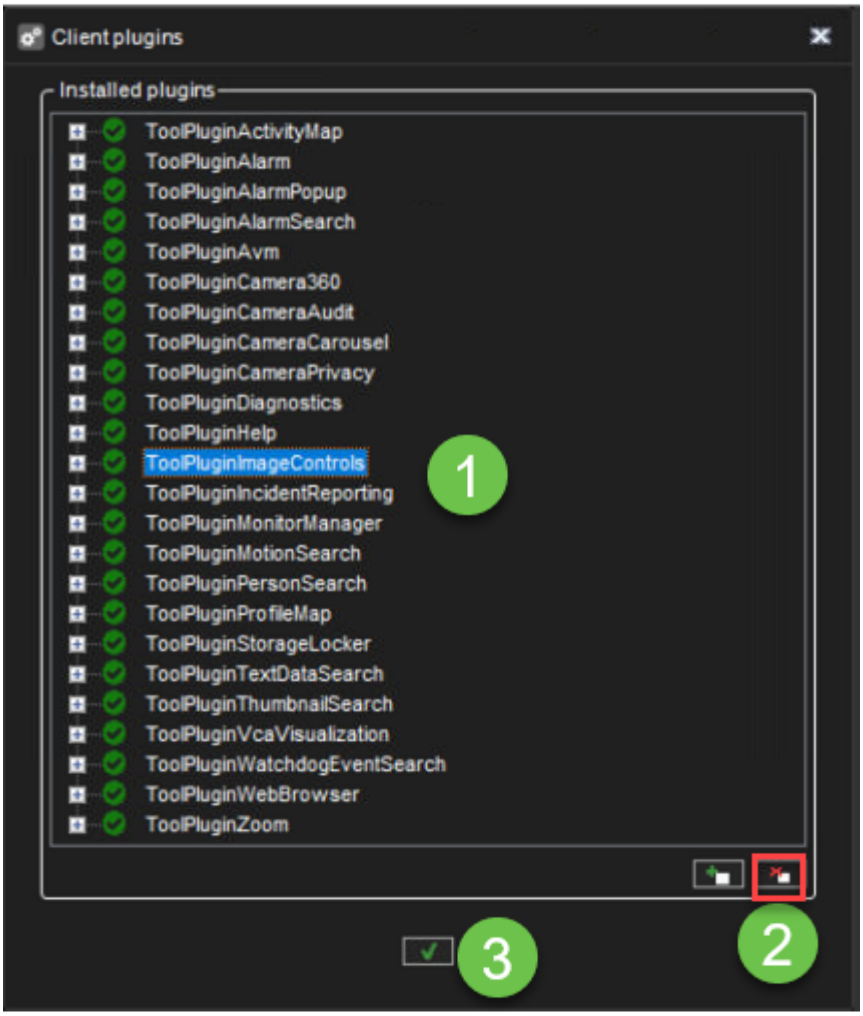


- Find and select the plugin package (.zip file) and click **OK**. The **Install Plugin** dialogue box is shown.
- If you want to force the system to install the driver package version, select **Install the driver even if the same or a newer version exists.**
- Click **Ok**

To remove a client plugin:

Open the **Install client plugin**

- Select plugin from the list
- Click **Remove client plugin**
- Click **Ok**



Client plugins

Installed plugins

- ToolPluginActivityMap
- ToolPluginAlarm
- ToolPluginAlarmPopup
- ToolPluginAlarmSearch
- ToolPluginAvm
- ToolPluginCamera360
- ToolPluginCameraAudit
- ToolPluginCameraCarousel
- ToolPluginCameraPrivacy
- ToolPluginDiagnostics
- ToolPluginHelp
- ToolPluginImageControls
- ToolPluginIncidentReporting
- ToolPluginMonitorManager
- ToolPluginMotionSearch
- ToolPluginPersonSearch
- ToolPluginProfileMap
- ToolPluginStorageLocker
- ToolPluginTextDataSearch
- ToolPluginThumbnailSearch
- ToolPluginVcaVisualization
- ToolPluginWatchdogEventSearch
- ToolPluginWebBrowser
- ToolPluginZoom

The VMS Servers

On the **VMS Servers** tab, you can configure these settings for each server:

Icon	Name	Description

⚙	General	Change the name and the description of the server. Here you will also find the IP address of the server.
⋖	Port forwarding	Users can see what the automatic port forwarding has configured as ports for this server. The ports can be changed if necessary.
🔲	Hardware	Add IP cameras and select camera and audio drivers.
📹	Cameras	Change camera parameters, recording schedules and motion detection settings.
🎤	Audio	Change audio detection settings and recording schedules.
⇄	Digital I/O	Set digital I/O settings.
🔔	Alarms	Set up alarm conditions and alarm actions.
☰	Storage	Add a hard disk to a server and set the storage times for video, audio, and alarm files.

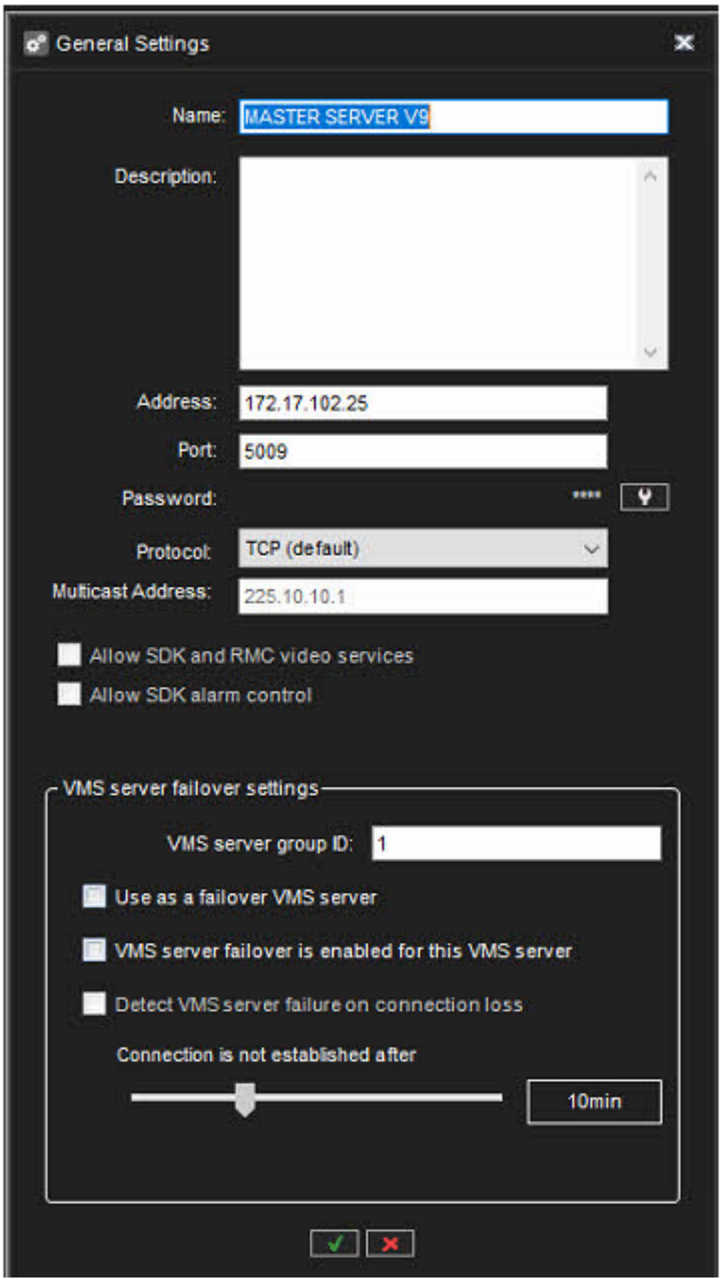
☰	Text channels	Set the names and descriptions of text data channels here.

To access the settings, do one of the following:

- Select the settings you want to configure (for example, Cameras) and then click Edit in the lower-right corner of the navigation pane.
- Double-click the settings that you want to configure.
- Drag the settings from the **VMS Servers** tab to the workspace.

General

1. VMS server name
2. Description
3. Password
4. Protocol
5. Multicast Address
6. VMS server failover settings



General Settings

Name: MASTER SERVER V9

Description:

Address: 172.17.102.25

Port: 5009

Password: ****

Protocol: TCP (default)

Multicast Address: 225.10.10.1

□ Allow SDK and RMC video services

□ Allow SDK alarm control

VMS server failover settings

VMS server group ID: 1

□ Use as a failover VMS server

□ VMS server failover is enabled for this VMS server

□ Detect VMS server failure on connection loss

Connection is not established after 10min

Multicast address

When a single workstation stream is opened multiple times, the server – and the network – face unnecessary strain as each stream is treated as a separate entity.

Multi-casting enables a single stream to be opened and sent to multiple workstations simultaneously.

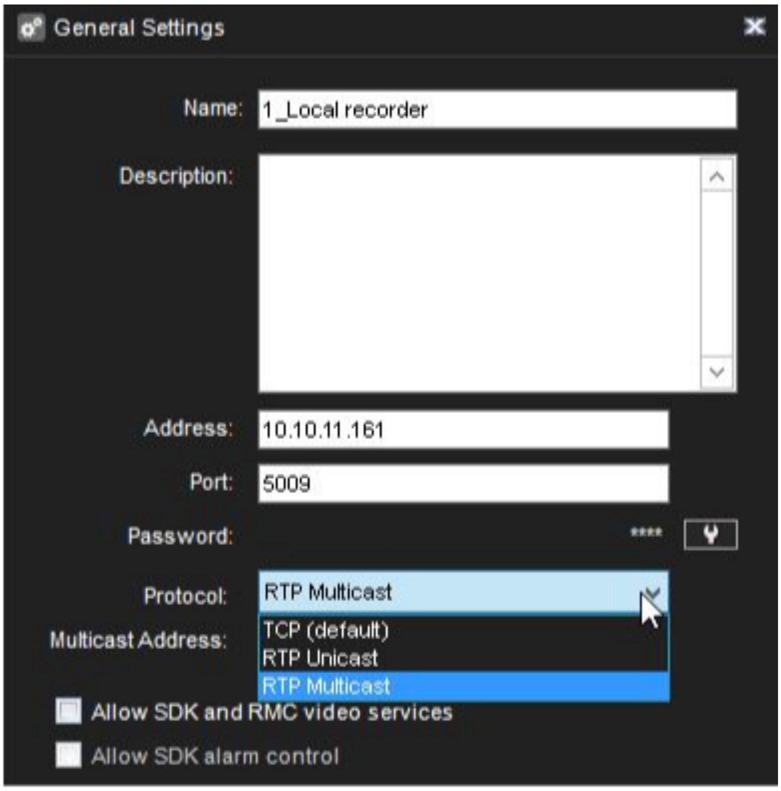
When using multi-casting, the stream for each video channel is sent to the LAN only once.

All applications on the LAN can receive the single stream, so network bandwidth usage is lower than when sending a stream for each application separately.

The feature needs to be configured in System Manager and through network settings.

Please refer to your network infrastructure service for information on enabling multi-casting support on the network level.

To configure multi-casting in System Manager:



General Settings

Name: 1_Local recorder

Description:

Address: 10.10.11.161

Port: 5009

Password: ****

Protocol: RTP Multicast

TCP (default)
RTP Unicast
RTP Multicast

Multicast Address:

□ Allow SDK and RMC video services

□ Allow SDK alarm control

- In the server’s General settings, change the protocol from **TCP (default)** to **RTP Multicast**.
- Edit the multicast address.
- Repeat steps 1-2 for all required servers in the system. Note: Each multicast address needs to be separate.

VMS server failover settings

When adding a new server to the system, it can be defined to be a failover server.

A failover server is a backup server that shall assume any server duties determined to be under failover protection.

Failover servers must have the same file system (same drive letters) as the VMS Servers under failover protection, and they can only be used for IP camera backup purposes.

When in standby mode, failover servers appear under a separate folder in the *VMS Server* list.

When any VMS Server is deemed to be broken or inaccessible, they have moved under the *"Broken VMS Servers"* folder.

Any available failover server shall take the responsibilities of the failed server.

Failover settings can be controlled from the general settings of the selected server.

The failover transition is done if all material disks are broken or the server is inaccessible for longer than a defined period.

Use as a failover VMS server

This setting define that the server is used as a failover VMS server

VMS Server failover is enabled for this VMS server

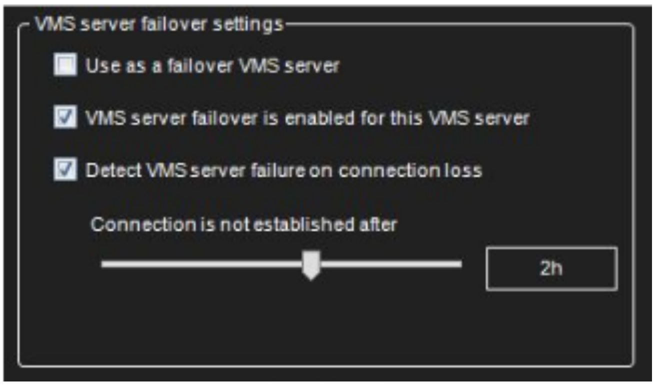
This setting defines the selected server role that will be transferred to the failover server during the error situation

Use automatic failback

This setting enables the automatic failback feature to this server

Use automatic material copying

This setting enables the automatic material copying feature to this server



VMS server failover settings

☐ Use as a failover VMS server

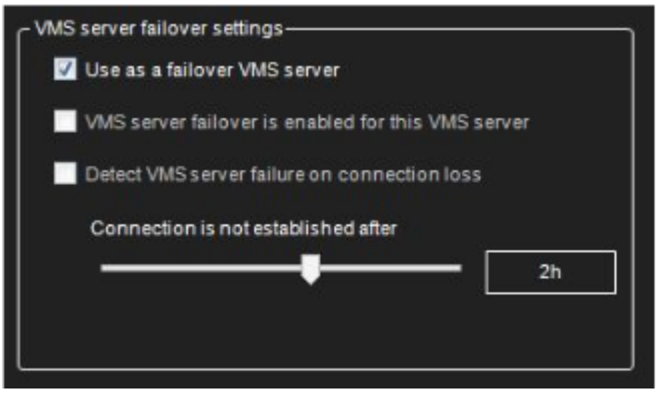
☑ VMS server failover is enabled for this VMS server

☑ Detect VMS server failure on connection loss

Connection is not established after

2h

For example, under failover protection, if inaccessible for longer than 2 hours, the failover switch would happen.



VMS server failover settings

☑ Use as a failover VMS server

☐ VMS server failover is enabled for this VMS server

☐ Detect VMS server failure on connection loss

Connection is not established after

2h

Port Forwarding

The basic idea with port forwarding is that it can access one or more VMS Servers or Master Servers behind a router that does Network Address Translation (NAT).

Typically, this situation happens when the client is outside the network and needs to access servers inside a company network.When installing a VMS Server, the installer offers the option to turn on the automatic port forwarding. The default state is off
If the port forwarding is not activated when the system is installed, it can be activated from the second tab, “VMS Servers”.
Open the view “Port forwarding” and activate the selection “UPnP is in use.”

Automatic Router Configuration

When a VMS Server starts up, it tries to discover UPnP devices from the network.
The router needs to support UPnP (Universal Plug and Play), which must be enabled on the device.
The server has continuous UPnP device discovery when running, so if any network changes are done, the server will automatically detect new routers and do port forwarding to them.
Only UPnP devices with external (WAN) addresses are detected.

If the user wants to remove port forwarding automatically, he can do this from the system manager. After this, the server will remember that the settings were removed and not port forward to this router.
The software does not allow to delete port forwarding mapping if the server is added to the system with an external address.

Deleting the port forward mapping would disconnect the system, and no further configuration would be possible.

If forward port settings are changed, and the connection to the server has not returned after a while, it might be necessary to reboot the router.

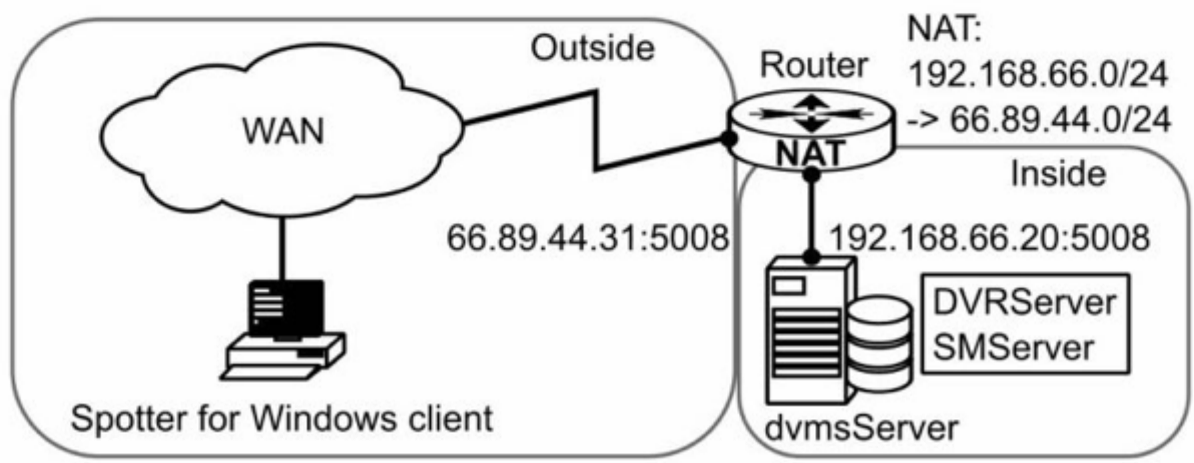
Servers need four ports for the server to server communication. The first server that does port forwarding will claim ports **5008**, **5009**, **5010** and **5011**.

The second server will claim ports **5012**-**5015**, the third server ports 5016-5019. And so on. (Assuming all the ports are available).

The first port is used for SMServer communication (**5008, 5012, 5016…**)
The second port is used for DVRServer process communication (**5009, 5013, 5017…**)
When connecting to a Master Server, the port is typically 5008. When adding new servers to the master, the port is typically 5009. If there are more than one server on-site, then the ports are 5009 +4, 5009 + 8 etc.

Single Server Behind Router

Scenario 1: Using a system with **a single server behind a router/firewall**

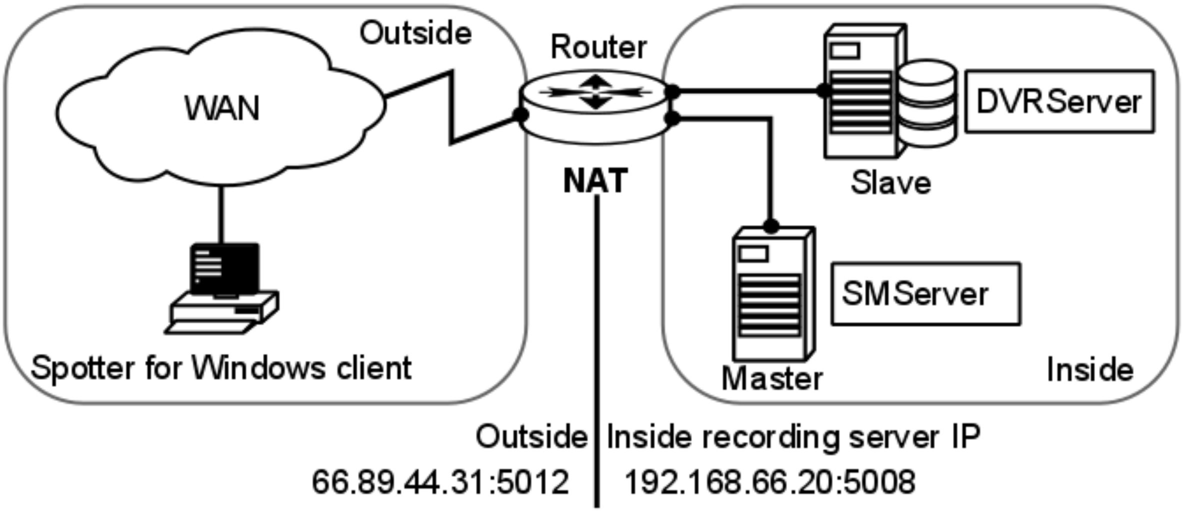


If the user is accessing a single server from the WAN, he needs to connect to the VMS Server with the outside IP address that the router has translated.

The user can check the port forwarding what the port in use is, but it is highly likely port 5008.

More Than One Server Behind Router

Scenario 2: More than one server behind a single router (WAN address)



If the user configures a more extensive system with multiple servers on a single site, he can add the servers to the System Manager application with the external or internal IP addresses.

When adding a new VMS Server, if the server has done automatic port forwarding, a note shows that he can choose between an internal IP address and an external IP address.

If the server is to be used from the WAN, then the external IP address should be chosen.

The exact ports that the server has done port forwarding to can be found by starting the System Manager on the local server.

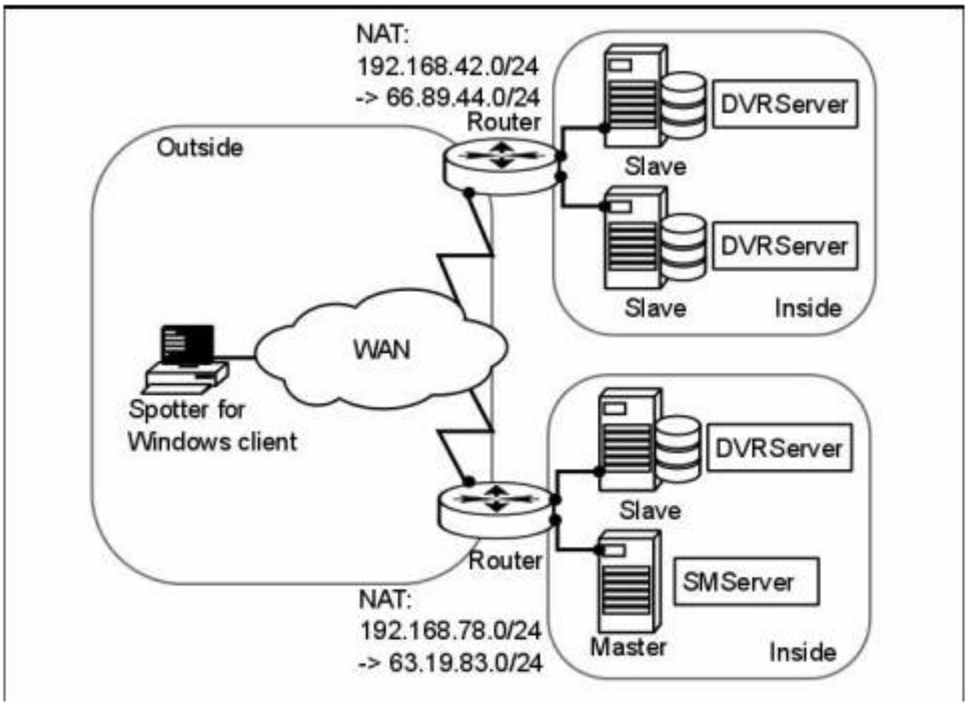
When adding a server to a Master Server when not on the local site (cannot use the local IP address), the user must know the external IP address and know the first port that the port forwarding was done to.

If the added server is a single, standalone server, the port is most likely 5009.

If multiple servers are on the same site, they most likely get the ports starting with **5009, 5013, 5017, 5021**…

More Than One Server On Multiple Sites

Scenario 3: More than one server on more than one site

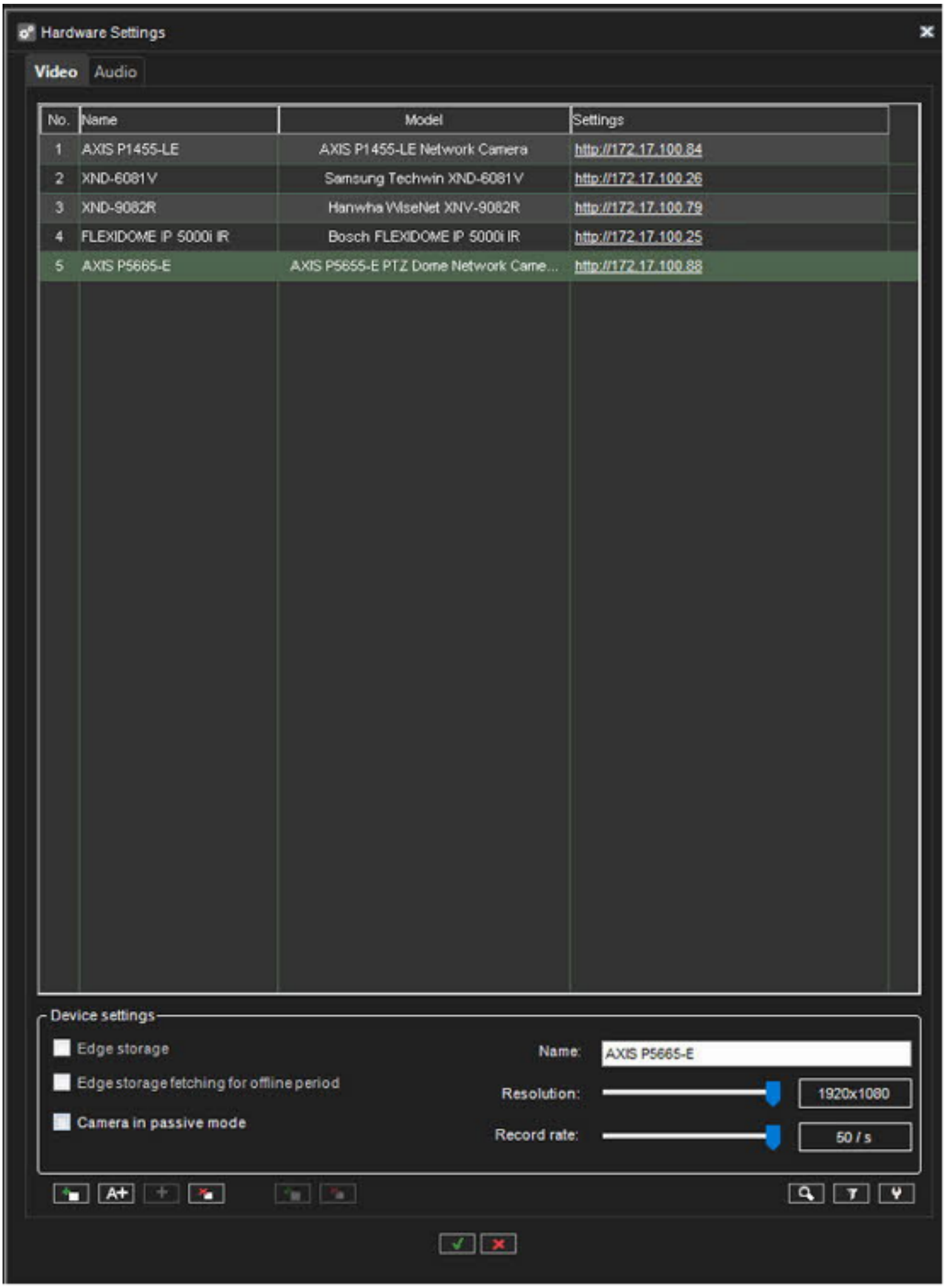


The same principle applies as in Scenario 2, but this time NAT needs to be taken into account when assigning VMS Servers to the Master Server from the other site.

Hardware

Before using the system manager application to search for the camera, please do the following actions:

1. Configure the IP address to the camera
2. Define the username and password to the IP cameras
3. Check that the camera time zone and time is the same as the VMS server



No.	Name	Model	Settings
1	AXIS P1455-LE	AXIS P1455-LE Network Camera	http://172.17.100.84
2	XND-6081V	Samsung Techwin XND-6081V	http://172.17.100.26
3	XND-9082R	Hanwha WiseNet XNV-9082R	http://172.17.100.79
4	FLEXIDOME IP 5000i IR	Bosch FLEXIDOME IP 5000i IR	http://172.17.100.25
5	AXIS P5665-E	AXIS P5665-E PTZ Dome Network Came...	http://172.17.100.88

Device settings

□ Edge storage

□ Edge storage fetching for offline period

□ Camera in passive mode

Name: AXIS P5665-E

Resolution: 1920x1080

Record rate: 50 / s

Also the information about used/total license count and information about used/total channels for selected multi-channel device were added below the "Devices" list in the "Hardware settings" dialog.

Video

When adding an IP camera, the following search modes are available.

1. ***All drivers***: Automatic search with all drivers. The system will attempt to use all available drivers. The mode option combo-box is disabled.
2. ***Selected drivers***: Automatic search with specific drivers only. The system will use only the drivers specified via the Selected Drivers dialogue during the automatic search.
   - The additional combo box will show all drivers that are currently selected. A user may use all of them (using the “All” option) or select only one driver.
3. ***Currently active drivers***: Search the camera using all drivers who are currently used. If this option is selected, the system will use only drivers currently used for already added cameras.
   a. For example, if we have Sony and Axis cameras subscribed, the search will be done by Sony and Axis drivers only.
   b. The mode option combo-box will contain a list of used drivers if the user wants to use one of them and an “All” option for using all drivers from this list for searching.
4. ***Driver***: Add a camera using a specific driver. The system will use only the specific driver for search.
   - The mode option combo-box will contain a list of all installed driver names to search.
   - If a search with specified drivers fails, the system will prompt whether the user wishes to search using all drivers.
   - The driver currently used for the search also should be excluded.
5. ***Camera model***: Add camera by model name. This mode is used for adding a camera by using an older capture driver using pre-defined capabilities from the driver configuration XML file.
   a. The mode option combo box will contain a list of available models.

The ***Selected drivers*** -mode will be selected by default for adding the new camera for the first time.

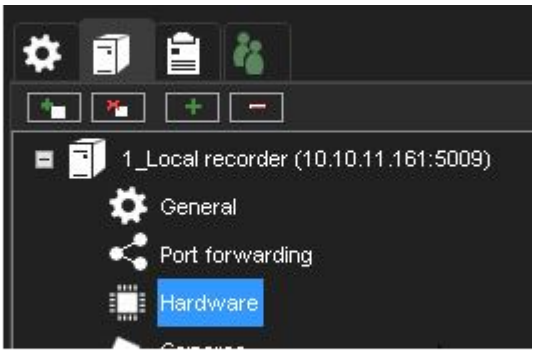
Next time the dialogue is opened, the system will remember the previous model and driver selection to allow the user to add similar cameras faster.

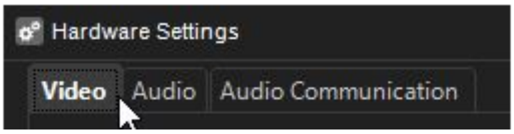
Opening the existing camera using the Modify button will show a dialogue with the Currently active drivers search mode and driver name in mode option combo-box (except cameras added by mod, el of course).

The system will not store last used options for modifying cases because the options will be available for adding cameras only

Add device

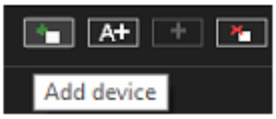
IP cameras or analogue video servers (encoders) can be managed through the **Video** tab of **Hardware settings**.





To add a new IP camera when the IP address is known:

1. On the **Video** tab, click **Add device**

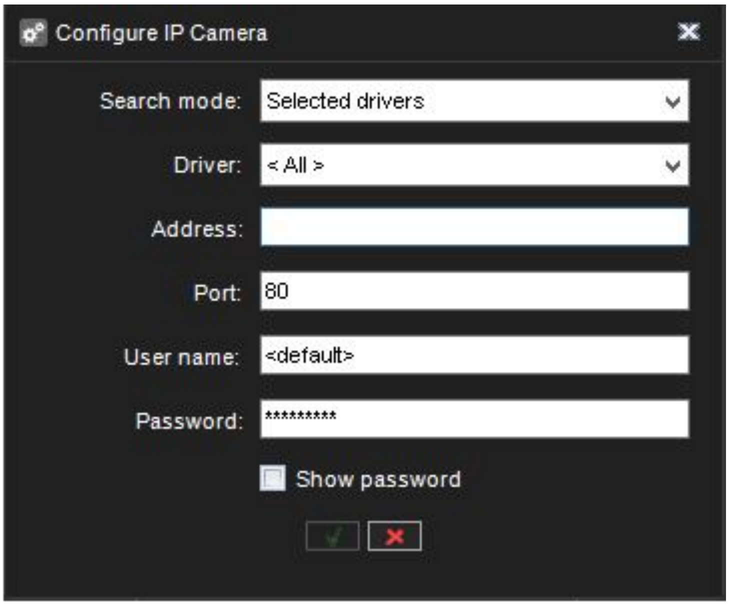


2. Type the IP address or DNS name of the camera or video server.

Change the port number if needed. Usually, port 80 is used.

3. Type the username and password for the camera.

4. Click **OK**.



Configure IP Camera

Search mode: Selected drivers

Driver: < All >

Address:

Port: 80

User name: <default>

Password: *********

□ Show password

The system will now communicate with the camera and display which drivers can connect to the camera.

The camera may support **ONVIF**. In this case, the **ONVIF** driver may also detect it.

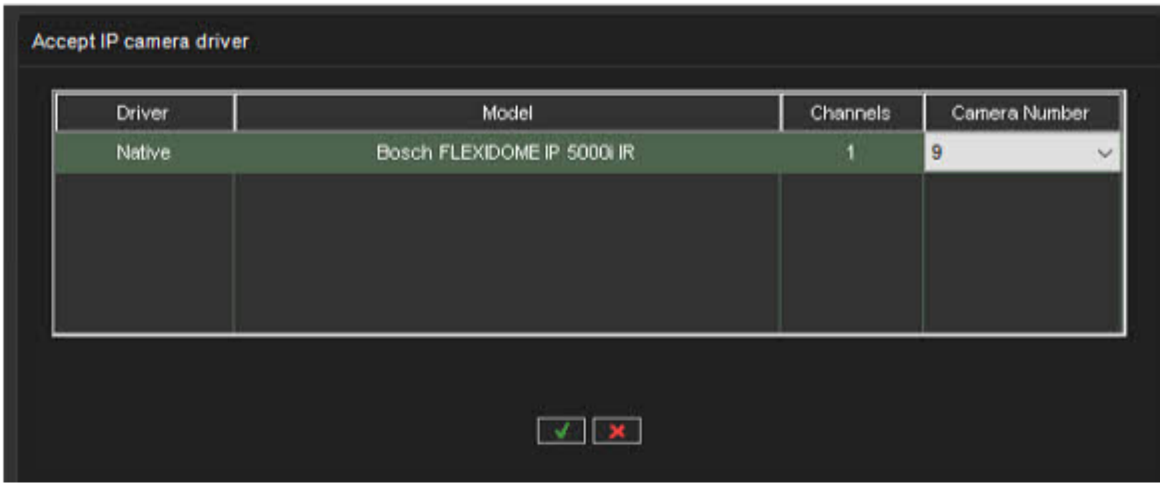
5. Select a driver from the list.

Typically, it is recommended to use the **Native** driver if it exists.

For multichannel devices, the **Channels** option can add the device with less than the maximum number of channels.

The user can also see what will be device camera number

6. Click **OK**

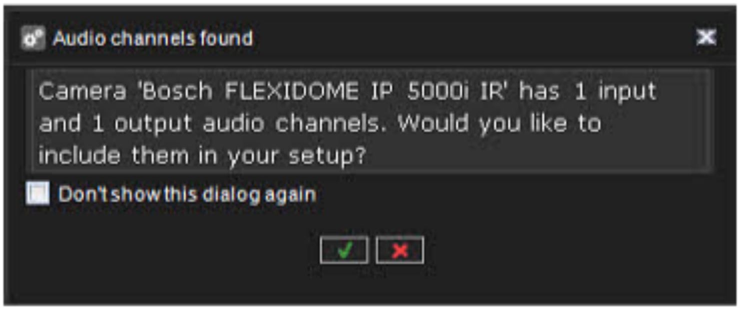


Accept IP camera driver

Driver	Model	Channels	Camera Number
Native	Bosch FLEXIDOME IP 5000i IR	1	9

If the camera supports audio channels, you will see dialogue about this.

7. Click **OK** to add also audio channels or **X** add an only video channel

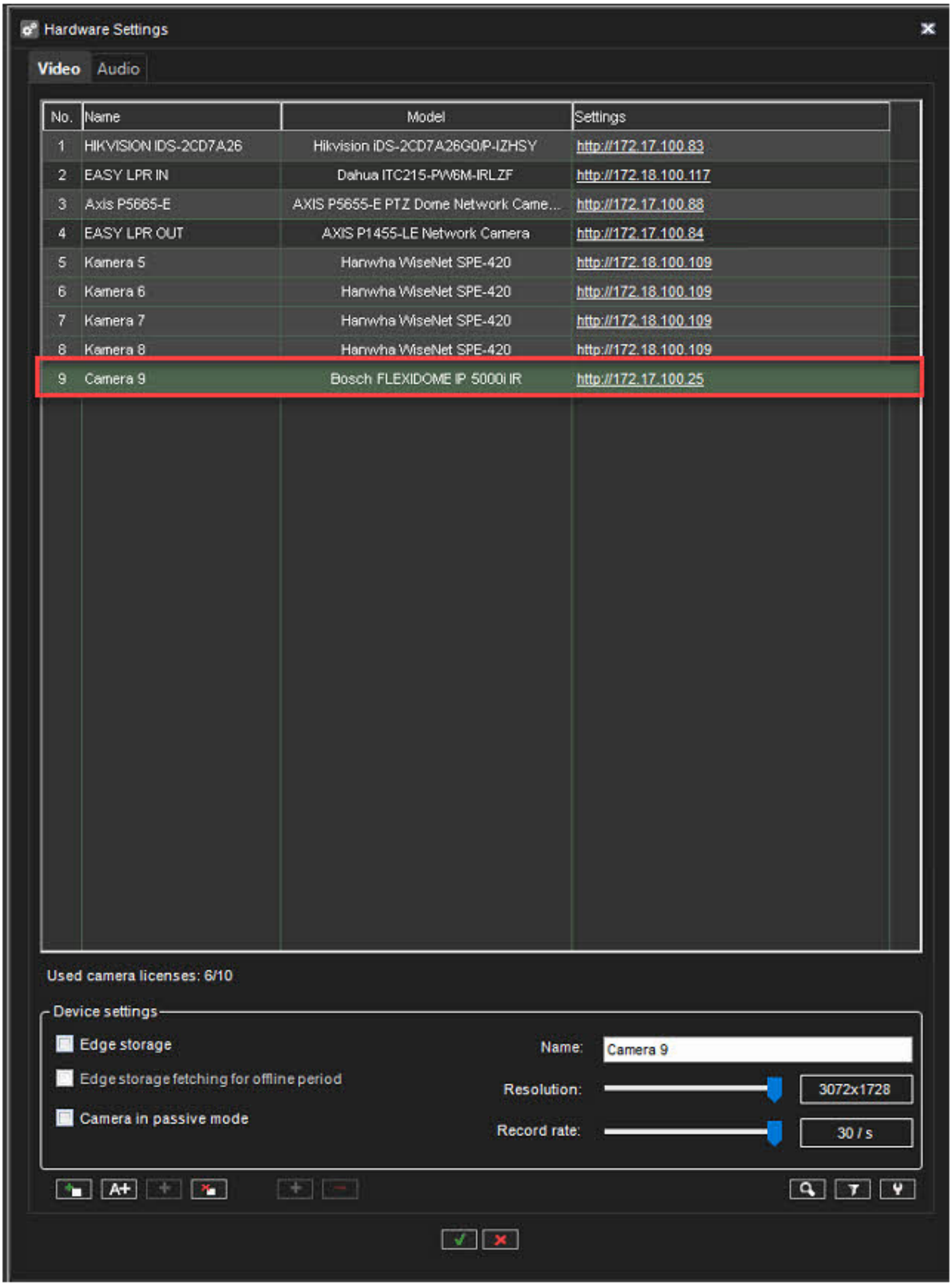


Audio channels found

Camera 'Bosch FLEXIDOME IP 5000i IR' has 1 input and 1 output audio channels. Would you like to include them in your setup?

□ Don't show this dialog again

After the camera adding device can be found from the **Hardware settings** list



No.	Name	Model	Settings
1	HIKVISION IDS-2CD7A26	Hikvision iDS-2CD7A26G0/P-IZHSY	http://172.17.100.83
2	EASY LPR IN	Dahua ITC215-PW6M-IRLZF	http://172.18.100.117
3	Axis P5665-E	AXIS P5655-E PTZ Dome Network Came...	http://172.17.100.88
4	EASY LPR OUT	AXIS P1455-LE Network Camera	http://172.17.100.84
5	Kamera 5	Hanwha WiseNet SPE-420	http://172.18.100.109
6	Kamera 6	Hanwha WiseNet SPE-420	http://172.18.100.109
7	Kamera 7	Hanwha WiseNet SPE-420	http://172.18.100.109
8	Kamera 8	Hanwha WiseNet SPE-420	http://172.18.100.109
9	Camera 9	Bosch FLEXIDOME IP 5000i IR	http://172.17.100.25

Used camera licenses: 6/10

Device settings

□ Edge storage

□ Edge storage fetching for offline period

□ Camera in passive mode

Name: Camera 9

Resolution: 3072x1728

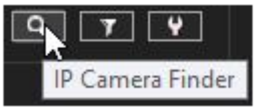
Record rate: 30 / s

New device can be inserted to the empty "slot" if its number of channels is the same or less then number of consecutive "not used" camera numbers.

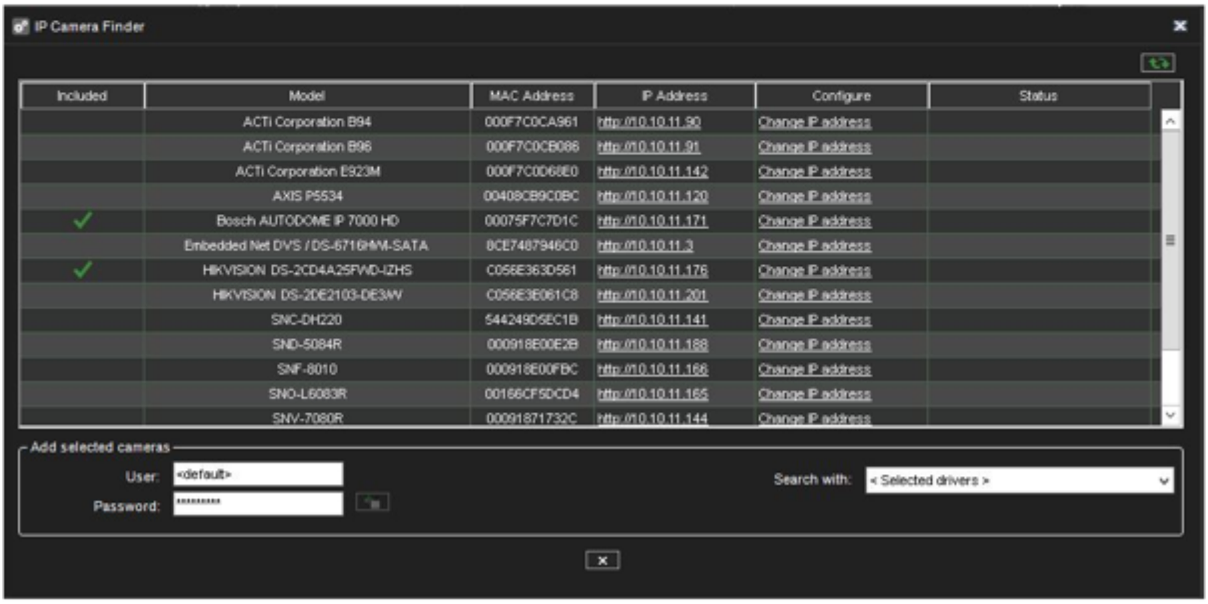
User can select channels that will be added during device acceptance. When he start device search and device is found, he will see the following dialog:

IP Camera Finder

1. Click the **IP camera finder**



The system will now scan the local IP network for active IP addresses and then communicate with each found IP address if it is a supported IP camera.
The resulting list is displayed after the search is complete.



Included	Model	MAC Address	IP Address	Configure	Status
	ACTi Corporation B94	000F7C0CA961	http://10.10.11.90	Change IP address	
	ACTi Corporation B96	000F7C0CB086	http://10.10.11.91	Change IP address	
	ACTi Corporation E923M	000F7C0D68E0	http://10.10.11.142	Change IP address	
	AXIS P5534	00408CB9C0BC	http://10.10.11.120	Change IP address	
✓	Bosch AUTODOME IP 7000 HD	00075F7C7D1C	http://10.10.11.171	Change IP address	
	Embedded Net DVS / DS-6716HW-SATA	8CE7487946C0	http://10.10.11.3	Change IP address	
✓	HIKVISION DS-2CD4A25FWD-IZHS	C056E363D561	http://10.10.11.176	Change IP address	
	HIKVISION DS-2DE2103-DE3W	C056E3E061C8	http://10.10.11.201	Change IP address	
	SNC-DH220	544249D5EC1B	http://10.10.11.141	Change IP address	
	SND-5084R	000918E00E2B	http://10.10.11.188	Change IP address	
	SNF-8010	000918E00FBC	http://10.10.11.166	Change IP address	
	SNO-L6083R	00166CF5DCD4	http://10.10.11.165	Change IP address	
	SNV-7080R	00091871732C	http://10.10.11.144	Change IP address	

Add selected cameras

User: <default>

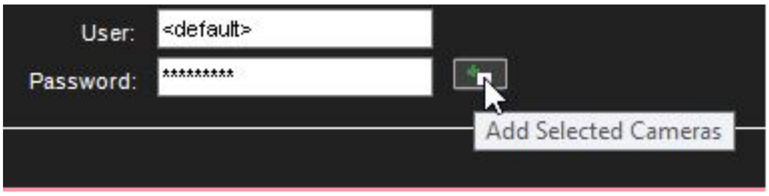
Password: *********

Search with: < Selected drivers >

Cameras can be selected from the list. Selecting multiple cameras is possible with SHIFT or CTRL keys.

1. Type the username and password for the cameras.

2. Click **Add Selected Cameras**.



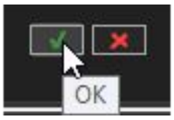
User: <default>
Password: *********

3. The system adds the selected cameras to the system with the selected username and password.

4. If the system cannot add some of the selected cameras, an error status message is displayed in the **Status** column; you can repeat steps 4-5 for the cameras with the correct credential information.

5. Click **Close** to exit the **IP camera finder**.

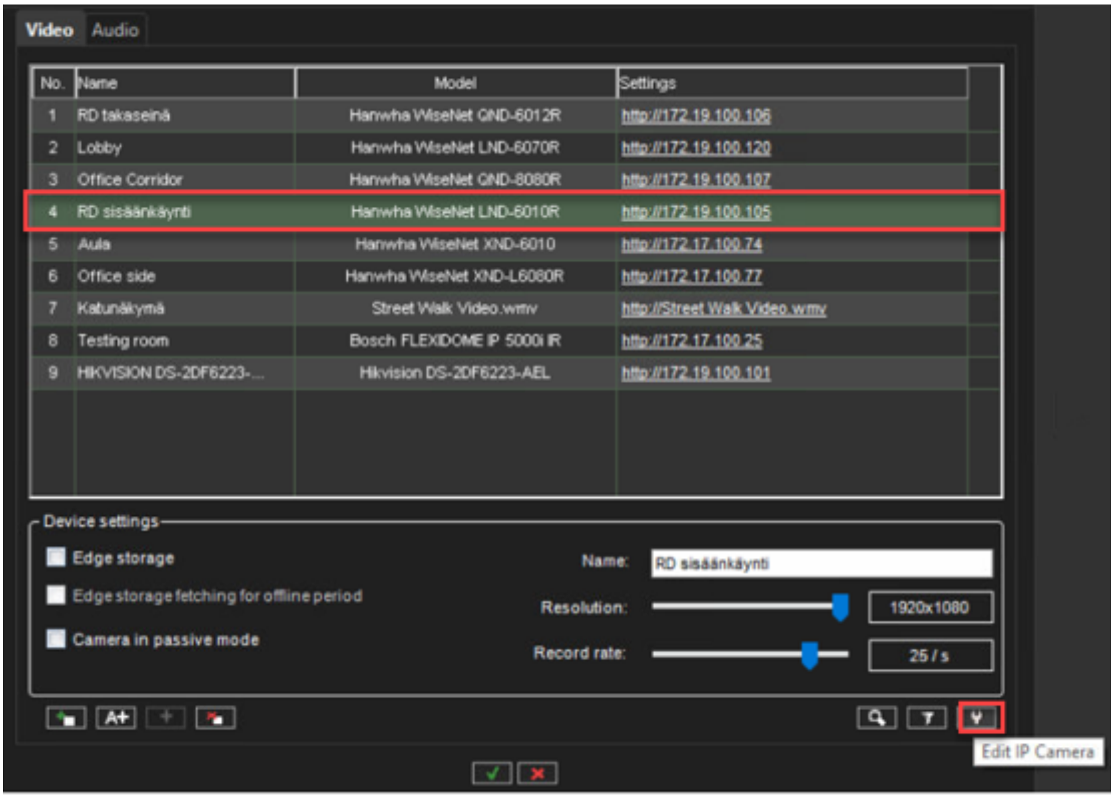
6. Save the Hardware settings by pressing **OK** in the list:



Edit IP Camera

Edit IP Camera allows users to change **camera address, port, username or password**

1. Select camera from the list
2. Click **Edit IP Camera**



No.	Name	Model	Settings
1	RD takaseinä	Hanwha WiseNet QND-6012R	http://172.19.100.106
2	Lobby	Hanwha WiseNet LND-6070R	http://172.19.100.120
3	Office Corridor	Hanwha WiseNet QND-8080R	http://172.19.100.107
4	RD sisäänkäynti	Hanwha WiseNet LND-6010R	http://172.19.100.105
5	Aula	Hanwha WiseNet XND-6010	http://172.17.100.74
6	Office side	Hanwha WiseNet XND-L6080R	http://172.17.100.77
7	Katunäkymä	Street Walk Video.wmv	http://Street Walk Video.wmv
8	Testing room	Bosch FLEXIDOME IP 5000i IR	http://172.17.100.25
9	HIKVISION DS-2DF6223-...	Hikvision DS-2DF6223-AEL	http://172.19.100.101

Device settings

□ Edge storage

□ Edge storage fetching for offline period

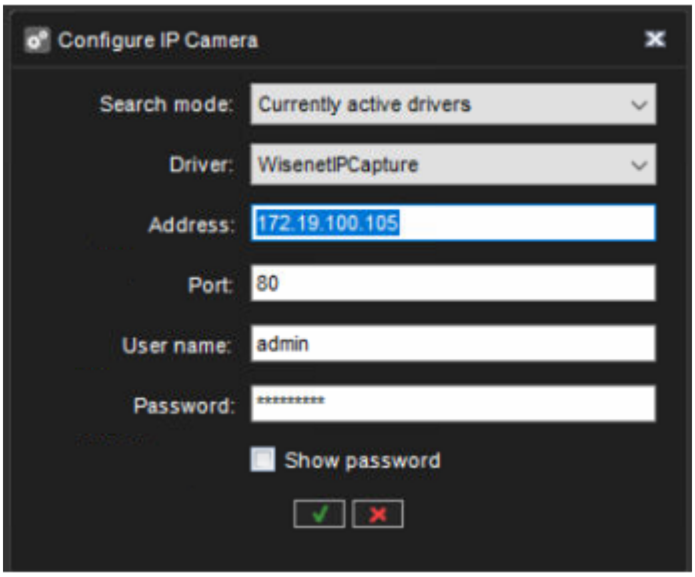
□ Camera in passive mode

Name: RD sisäänkäynti

Resolution: 1920x1080

Record rate: 25 / s

1. Do needed modifications
2. Click Ok to confirm changes


Configure IP Camera

Search mode: Currently active drivers

Driver: WisenetIPCapture

Address: 172.19.100.105

Port: 80

User name: admin

Password: *********

□ Show password

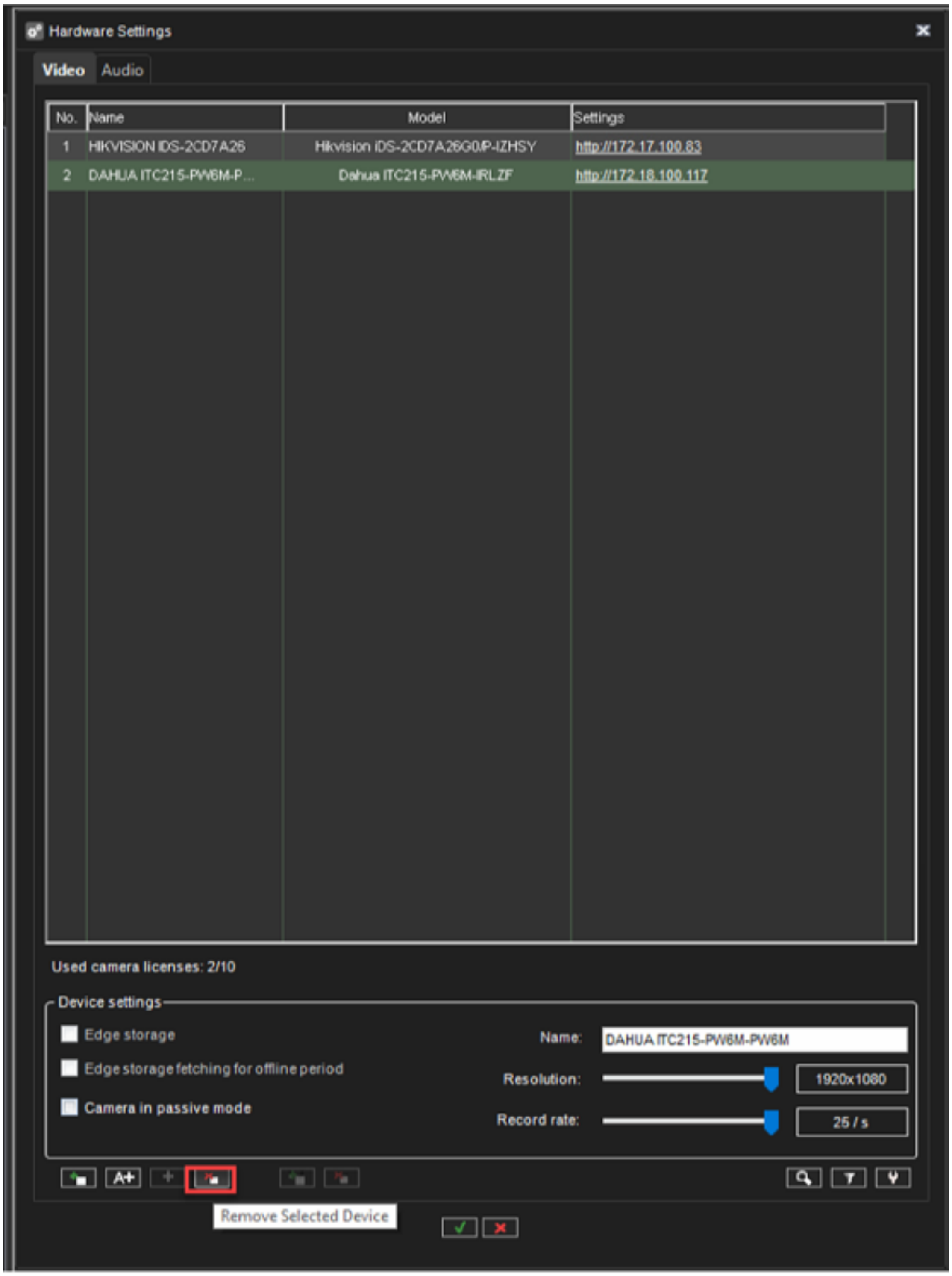
Removing IP cameras and encoders

If you open the "**Hardware Settings**" dialogue in System Manager, you will see 2 buttons below the list of cameras:

1. The "**Add video channel to the selected device**" button
2. The "**Remove video channel from the selected device**" button

To remove an IP camera:

1. Select camera from the list on the **Video** tab
2. Click **Remove Selected Device** in the lower right corner of the tab.
3. When asked to confirm the deletion, click **OK**.



No.	Name	Model	Settings
1	HIKVISION IDS-2CD7A26	Hikvision iDS-2CD7A26G0/P-IZHSY	http://172.17.100.83
2	DAHUA ITC215-PW6M-P...	Dahua ITC215-PW6M-IRLZF	http://172.18.100.117

Used camera licenses: 2/10

Device settings

□ Edge storage

□ Edge storage fetching for offline period

□ Camera in passive mode

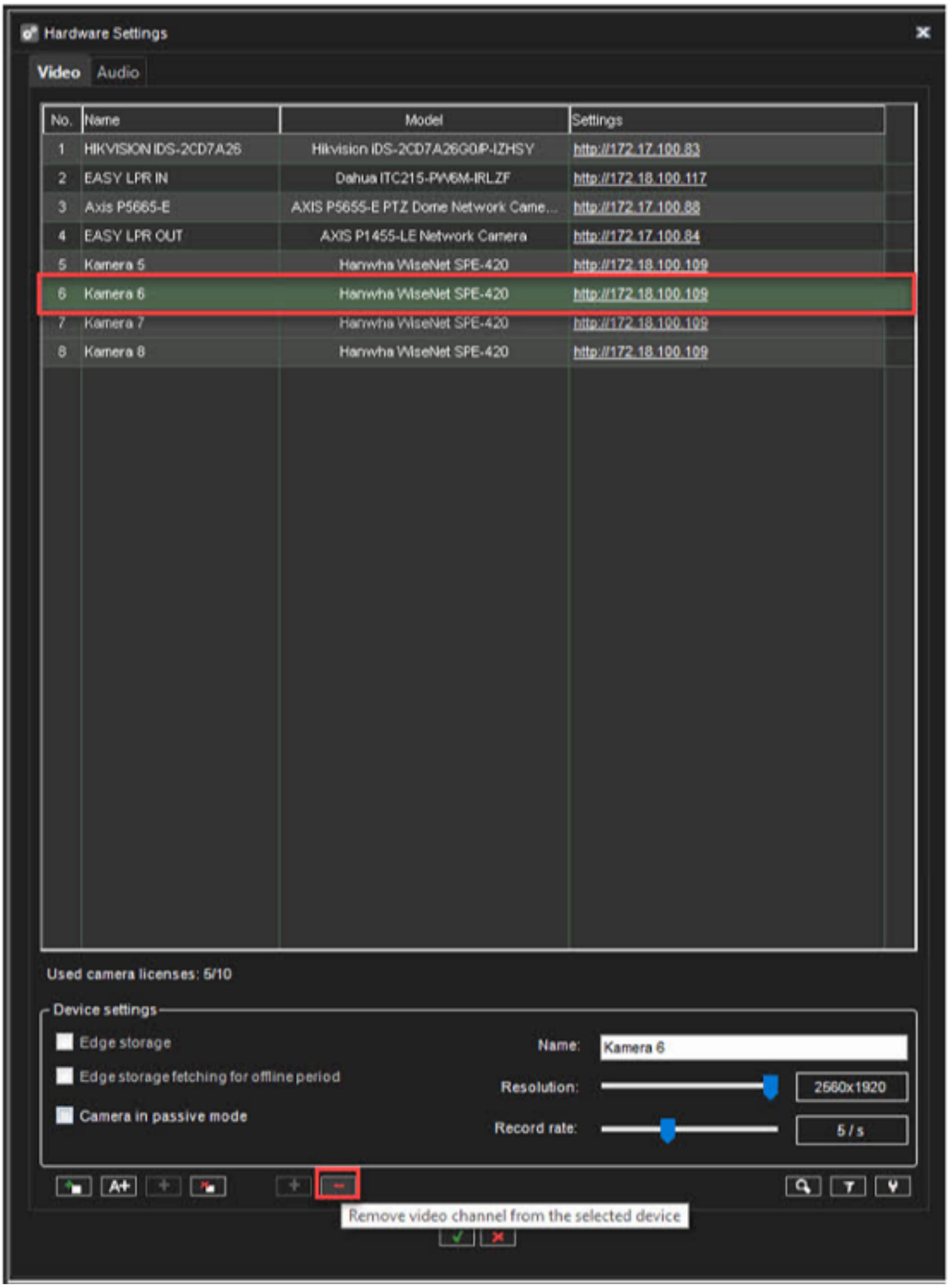
Name: DAHUA ITC215-PW6M-PW6M

Resolution: 1920x1080

Record rate: 25 / s

To remove video channels from the encoder or multi-lens cameras:

1. Select the correct channel from the list
2. Click **Remove video channel from the selected device**
3. Click **OK**



Hardware Settings

Video Audio

No.	Name	Model	Settings
1	HIKVISION IDS-2CD7A26	Hikvision iDS-2CD7A26G0/P-IZHSY	http://172.17.100.83
2	EASY LPR IN	Dahua ITC215-PW6M-IRLZF	http://172.18.100.117
3	Axis P5665-E	AXIS P5655-E PTZ Dome Network Came...	http://172.17.100.88
4	EASY LPR OUT	AXIS P1455-LE Network Camera	http://172.17.100.84
5	Kamera 5	Hanwha WiseNet SPE-420	http://172.18.100.109
6	Kamera 6	Hanwha WiseNet SPE-420	http://172.18.100.109
7	Kamera 7	Hanwha WiseNet SPE-420	http://172.18.100.109
8	Kamera 8	Hanwha WiseNet SPE-420	http://172.18.100.109

Used camera licenses: 5/10

Device settings

□ Edge storage

□ Edge storage fetching for offline period

□ Camera in passive mode

Name: Kamera 6

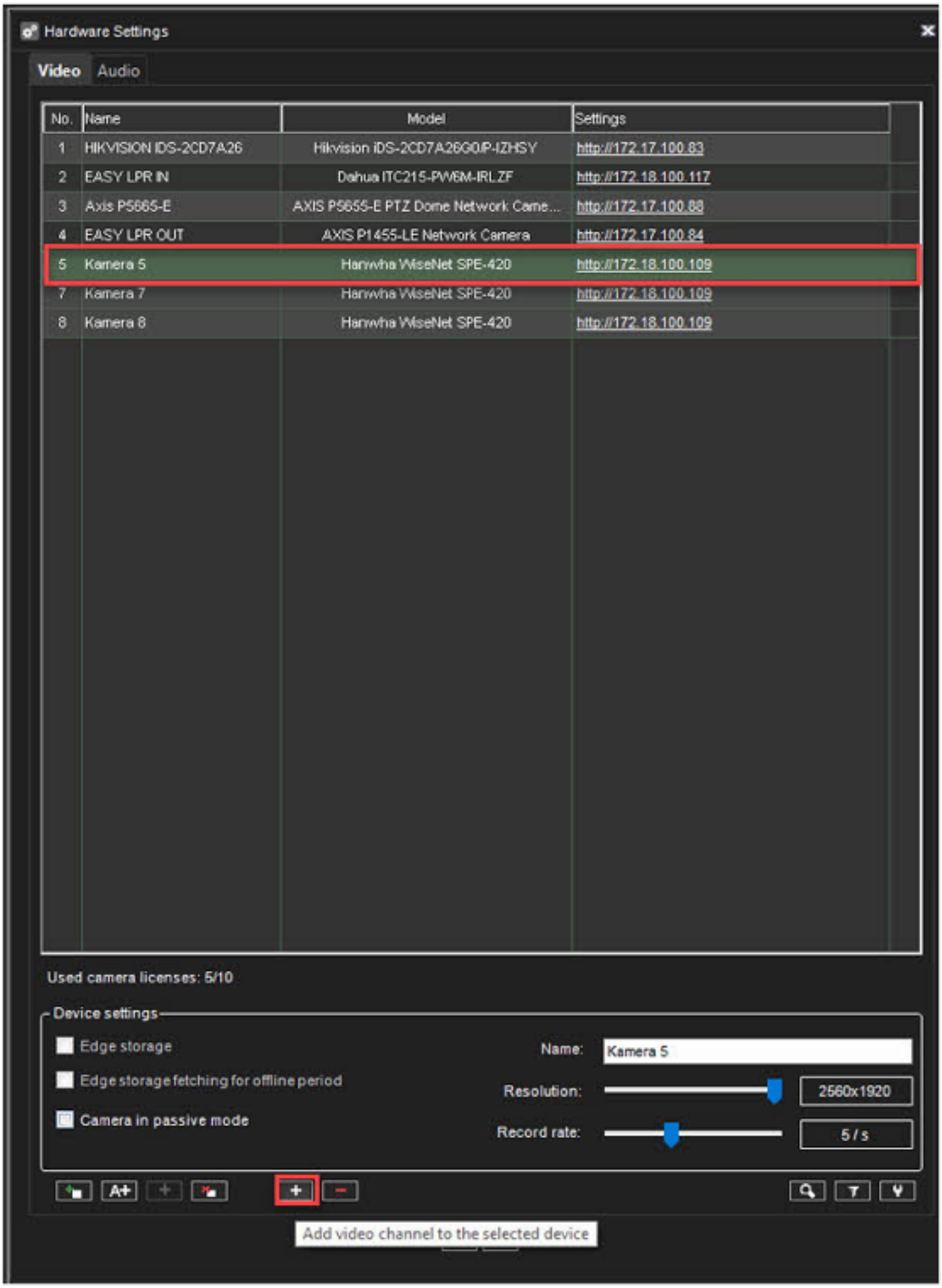
Resolution: 2560x1920

Record rate: 5 / s

Remove video channel from the selected device

To add video channels to the encoder or multi-lens cameras:

1. Select the correct device from the list
2. Click **Add video channel to the selected device**
3. Click **OK**



No.	Name	Model	Settings
1	HIKVISION IDS-2CD7A26	Hikvision iDS-2CD7A26G0/P-IZHSY	http://172.17.100.83
2	EASY LPR IN	Dahua ITC215-PW6M-IRLZF	http://172.18.100.117
3	Axis P5665-E	AXIS P5655-E PTZ Dome Network Came...	http://172.17.100.88
4	EASY LPR OUT	AXIS P1455-LE Network Camera	http://172.17.100.84
5	Kamera 5	Hanwha WiseNet SPE-420	http://172.18.100.109
7	Kamera 7	Hanwha WiseNet SPE-420	http://172.18.100.109
8	Kamera 8	Hanwha WiseNet SPE-420	http://172.18.100.109

Used camera licenses: 5/10

Device settings

□ Edge storage

□ Edge storage fetching for offline period

□ Camera in passive mode

Name: Kamera 5

Resolution: 2560x1920

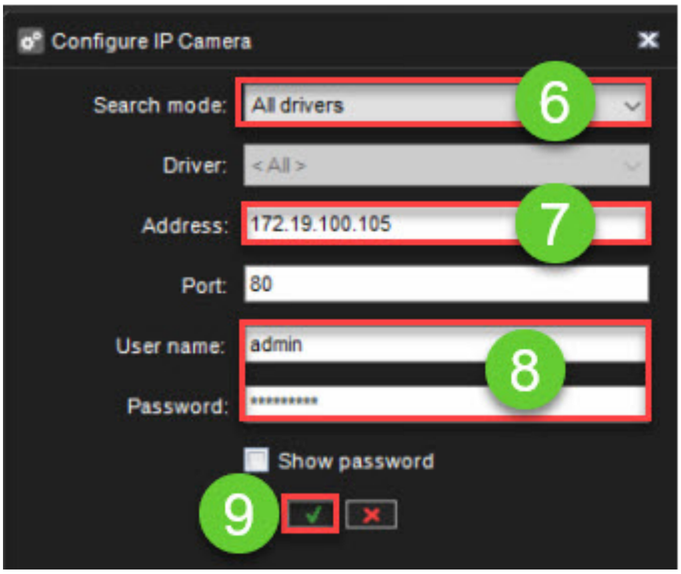
Record rate: 5 / s

Add video channel to the selected device

The user can replace an existing IP camera in the Mirasys VMS

- Add an existing IP camera address to the new IP camera
- Set same username and password to the new IP camera
- Connect camera to the network
- Select camera from the **Hardware** list
- Click **Edit IP camera**

1. Select **Search mode: All drivers**
2. Check that camera has correct IP address
3. Check that username and password are correct
4. Click **OK**
5. Select the correct driver from the **Accept IP camera driver** selection
6. Click **OK**



Configure IP Camera

Search mode: All drivers

Driver: < All >

Address: 172.19.100.105

Port: 80

User name: admin

Password: **********

□ Show password

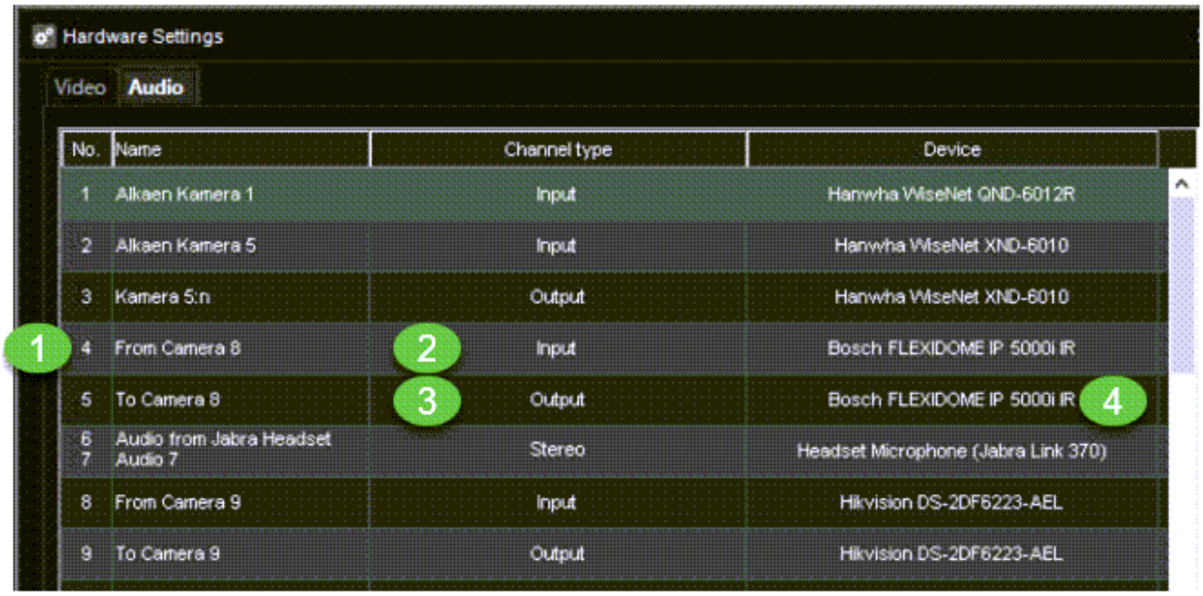
Audio

If a camera has compatible IP audio input or output channels, you can add them simultaneously when adding the camera through the automated search tools.

After IP audio inputs and outputs for a camera have been added to the system, they can be edited and removed through the **Audio** tab.

Information shown:

1. Camera hardware ID
2. Channel type(Input)
3. Channel type(Output(
4. Device model



No.	Name	Channel type	Device
1	Alkaen Kamera 1	Input	Hanwha WiseNet QND-6012R
2	Alkaen Kamera 5	Input	Hanwha WiseNet XND-6010
3	Kamera 5:n	Output	Hanwha WiseNet XND-6010
4	From Camera 8	Input	Bosch FLEXIDOME IP 5000i IR
5	To Camera 8	Output	Bosch FLEXIDOME IP 5000i IR
6 7	Audio from Jabra Headset Audio 7	Stereo	Headset Microphone (Jabra Link 370)
8	From Camera 9	Input	Hikvision DS-2DF6223-AEL
9	To Camera 9	Output	Hikvision DS-2DF6223-AEL

Device Settings

Edge Storage

The Edge storage functionality enables uninterrupted recording during network blackouts. In practice, in-network blackout, the video feed can be stored on an SD memory card on the camera. Once the network connection has been re-established, video is transmitted from the camera’s SD card to the server.

Please refer to the camera manufacturer documentation to see what cameras support the feature.

Edge storage must be enabled in the device settings.

This feature is configured solely through the camera’s configuration utility.

Please refer to the camera’s documentation for instructions on enabling Edge storage.

Edge storage fetching for offline period

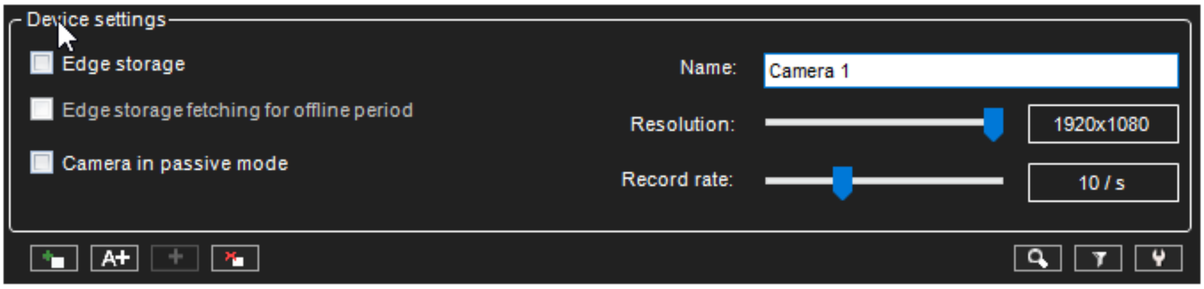
When this is enabled, then Mirasys VMS transfers recordings from the camera SD card only from the time of the period, when the connection has been lost between the Mirasys VMS and IP camera

Camera in passive mode

1. If multiple servers have the same camera configured, then one should be made **Active,** and the others should be **Passive**.
2. This way, only the Active server settings are communicated to the camera.

Camera information

Camera name, resolution and record rate can be set directly from the **Video** tab



Device settings

□ Edge storage

□ Edge storage fetching for offline period

□ Camera in passive mode

Name: Camera 1

Resolution: 1920x1080

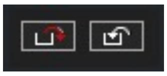
Record rate: 10 / s

Adding cameras by using CSV file

VSM camera settings can be exported to a CSV file and imported to VMS from a CSV file. This allows administrators to make bulk changes to camera settings and then import changed settings to the VMS system. It is also possible to add new cameras to VMS using this functionality.

CSV file import and export

System Manager Hardware settings have the following buttons for exporting camera settings to a file and importing camera settings from a file in CSV format.



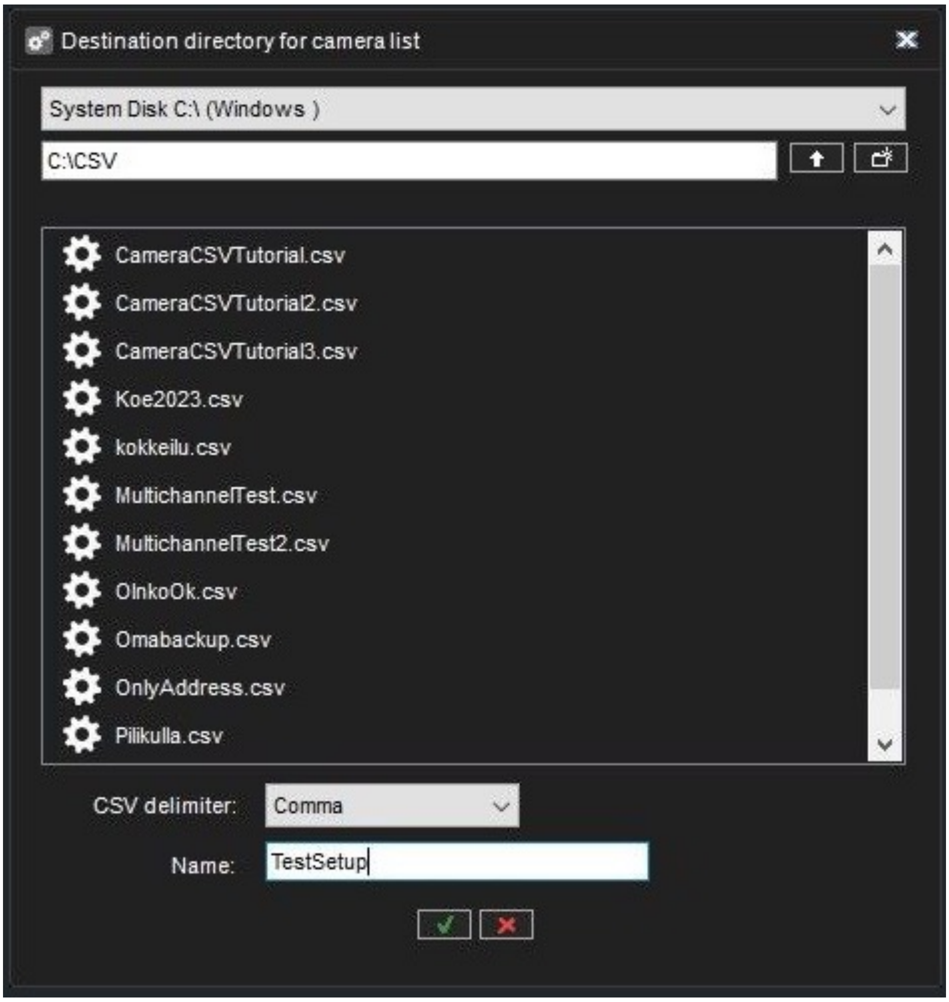
CSV file format

CSV file format for each camera uses the following header names.

- **Name** - Name of the camera channel.
- **Number** - Number of the camera channel on the VMS server.
- **Description** - Camera channel description.
- **AdmDescription** - Camera channel administrative description.
- **Address** - Camera device address.
- **Port** - Camera device port.
- **UserName** - Camera device user name.
- **Password** - Camera device password.
- **Driver** - Driver name / native (search from all available native drivers) / ONVIF (use of ONVIF driver). Logic uses the first driver that includes the given driver name string. For example, axis → NewAxisIPCapture.
- **Channel** - Used channel of the driver if the device supports more than one channel. With one-channel devices, this can be left empty.
- **IsInUse** - Is the camera in use?
- **IsAudioInUse** - Is audio in use if the driver supports it?
- **IsIOInUse** - Is I/O in use. This has meaning only when exporting CSV files. At import, I/O is used automatically if the device supports it.
- **Is360** - Is 360 camera.
- **Framerate** - Recording stream frames / second rounded to close available value. The header for other streams: Framerate1, Framerate2, Framerate3.
- **Resolution** - Recording stream resolution in format width x height (for example 1920x1080) rounded to close available value. For other streams: Resolution1, Resolution2, Resolution3.
- **Codec** - Recording stream used compression codec. Rounded to close available value: JPEG, MPEG, H264, WMC9, PARSE, H265, MXPEG. For other streams: Codec1, Codec2, Codec3.
- **Quality** - Recording stream compression quality rounded to close available value in range 1-100. For other streams: Quality1, Quality2, Quality3.
- **Bitrate** - Recording stream bit rate rounded to close available value. For other streams: Bitrate1, Bitrate2, Bitrate3.

Export

Users can select the folder where the camera settings CSV file is exported to and give the name of the file. Users can also define the delimiter that is used in the CSV file.



Destination directory for camera list

System Disk C:\ (Windows)

C:\CSV

- CameraCSVTutorial.csv
- CameraCSVTutorial2.csv
- CameraCSVTutorial3.csv
- Koe2023.csv
- kokkeilu.csv
- MultichannelTest.csv
- MultichannelTest2.csv
- OlnkoOk.csv
- Omabackup.csv
- OnlyAddress.csv
- Pilikulla.csv

CSV delimiter: Comma

Name: TestSetup

When the export is successful, a blinking green icon is shown. In error, a blinking red icon is shown.

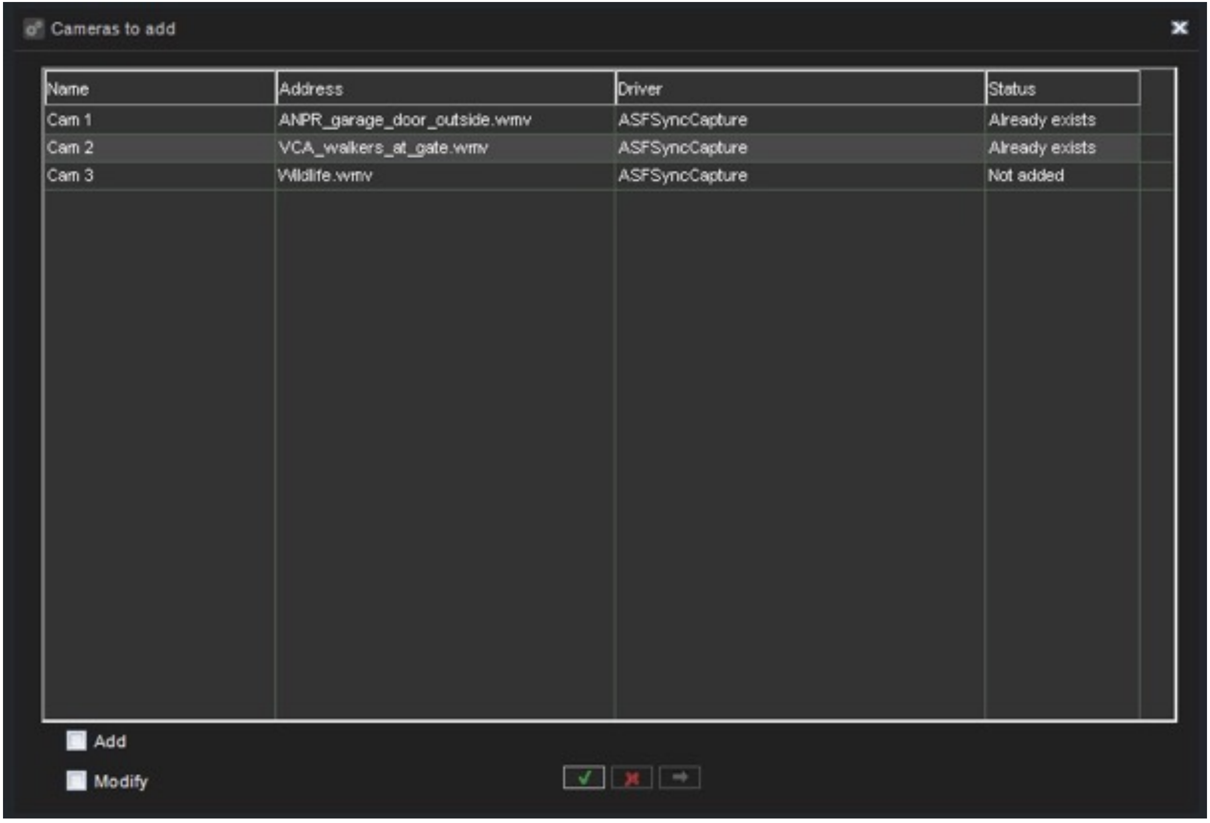
Import

When the user clicks the import button, the select file dialog is shown to select the CSV file to import. When the file is selected, the camera adding view is shown if CSV file parsing and validation are done successfully.

The following validation rules are used when parsing imported CSV files.

1. CSV file column delimiter is a comma (,) or semicolon (;).

2. The order of the header names (i.e. column order) is free.
3. Unused header names (i.e. columns) can be left off.
4. Only the Address header name is mandatory. If it is missing, CSV file data is not accepted.
5. If some property names and data do not exist, an internal default value is used.
6. For validation errors and warnings, a message popup is generated, and more information is printed in the System Manager log.



Name	Address	Driver	Status
Cam 1	ANPR_garage_door_outside.wmv	ASFSyncCapture	Already exists
Cam 2	VCA_walkers_at_gate.wmv	ASFSyncCapture	Already exists
Cam 3	Wildlife.wmv	ASFSyncCapture	Not added

□ Add
□ Modify

After the CSV file validation and parsing, the status column informs if the camera is already added to the system (Already exists) or if it is the new camera (Not added). Add and Modify check boxes appear if there are modifications to existing cameras and new camera configurations in the imported CSV file. These options can be used to select if cameras from the CSV file are added and/or modified. Execute button is enabled when there are cameras to be added or modified. By clicking the execute button, settings from the CSV file are applied (modified and/or added) to the current settings. After the settings apply, the status for each camera is updated, Dialog can be closed after the settings apply by clicking the ok button or from the cancel button before the settings apply. Modified camera settings and/or added cameras are applied to the VMS server once the hardware settings are saved.

Adding and Removing VMS Servers

You can have (depending on the license) from 1 to unlimited servers in one system.

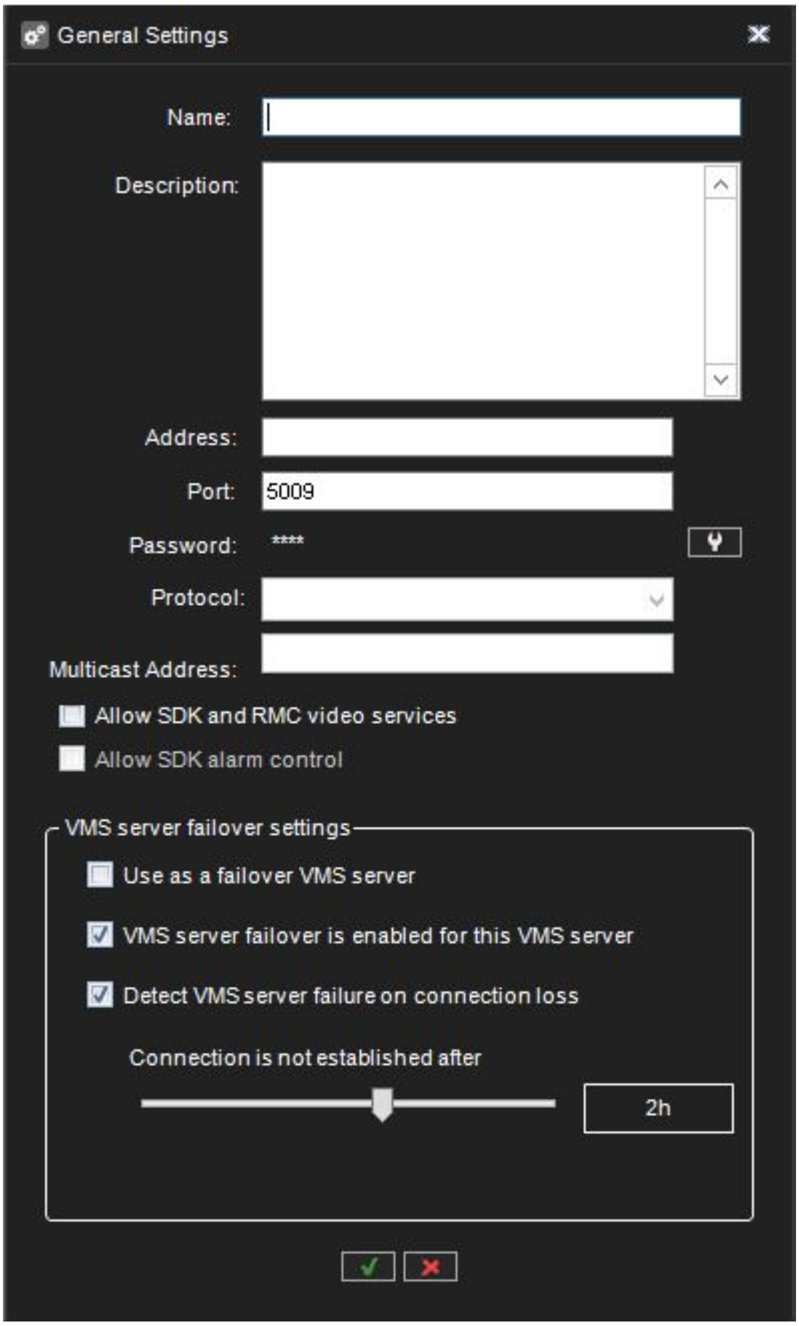
One server should not belong to more than one Master Server (SMServer).

You can specify a password for each server.

The system will prompt for the password if someone tries to add the server to another system.

To add a server to the system(recording server):

1. Open the **VMS Servers** tab
2. Click Add VMS Server
3. The **General Settings** dialogue box is shown.
4. Type name for the server
5. Enter a description, if needed
6. Type the IP address or DNS name of the server.
7. Enter the password for the server, if needed
8. Click **OK**. The server and the devices connected to it (cameras and audio channels) are added to the list.
    a. Note: *If the server is password-protected, the system prompts for the password.*



General Settings

Name:

Description:

Address:

Port: 5009

Password: ****

Protocol:

Multicast Address:

□ Allow SDK and RMC video services

□ Allow SDK alarm control

VMS server failover settings

□ Use as a failover VMS server

☑ VMS server failover is enabled for this VMS server

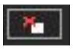
☑ Detect VMS server failure on connection loss

Connection is not established after

2h

To remove a server from the system:

1. Select the server that you want to remove.
2. Click Remove **VMS Server**



3. Click **OK** to confirm.

Connection status:

If the connection to the server is lost, the System Manager application will automatically try to connect to the server.

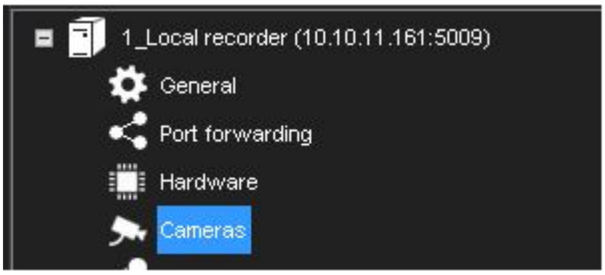
NOTE:

When you have added Mirasys VMS as a slave server, please do the following actions:

1. Change Admin user password using a slave server System Manager
2. Disable SMServer service from the slave server

Cameras

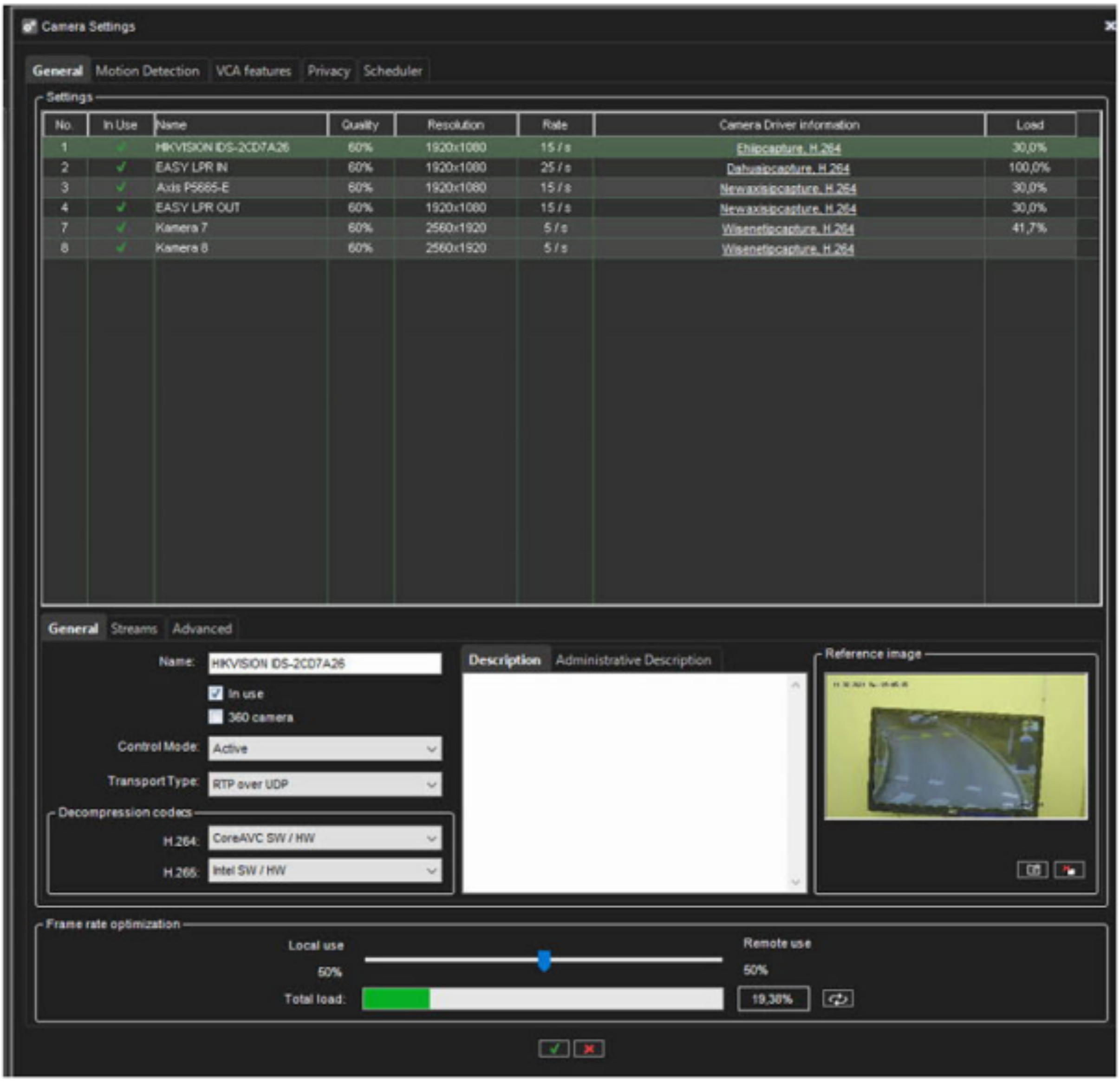
After the camera has been added to the server, the camera settings can be configured from the **Cameras** page.



Camera Settings contain settings for:

- General
- Motion Detection
- VCA features
- Privacy
- Scheduler

Camera settings



No.	In Use	Name	Quality	Resolution	Rate	Camera Driver information	Load
1	✓	HIKVISION IDS-2CD7A26	60%	1920x1080	15 / s	Ehipcapture, H.264	30,0%
2	✓	EASY LPR IN	60%	1920x1080	25 / s	Dahuaipcapture, H.264	100,0%
3	✓	Axis P5665-E	60%	1920x1080	15 / s	Newaxisipcapture, H.264	30,0%
4	✓	EASY LPR OUT	60%	1920x1080	15 / s	Newaxisipcapture, H.264	30,0%
7	✓	Kamera 7	60%	2560x1920	5 / s	Wisenetipcapture, H.264	41,7%
8	✓	Kamera 8	60%	2560x1920	5 / s	Wisenetipcapture, H.264	

Name: HIKVISION IDS-2CD7A26

☑ In use

☐ 360 camera

Control Mode: Active

Transport Type: RTP over UDP

Decompression codecs

H.264: CoreAVC SW / HW

H.265: Intel SW / HW

Local use 50%

Remote use 50%

Total load: 19,38%

General settings

Name

The name of the camera. The system suggests names of the type *Camera 1, Camera 2*, and so on.

In Use

Clear this check box if no camera is connected to the camera input or if you want to disable the camera.

360 camera.

This tells the Spotter client that the camera is a 360 camera, and Spotter will show the image de-warping options in the camera toolbar (if installed)

Control Mode

This setting has two options, **Active** (default) and **Passive**.
If multiple servers have the same camera configured, then one should be made **Active,** and the others should be **Passive**.
This way, only the Active server settings are communicated to the camera.

Transport Type

This setting controls how the media stream is transported from camera to server.
The available options are **RTP over UDP** (default) and **RTP over RTSP**.
If the camera seems to work poorly with one setting (for example, if there are holes in camera material or difficulty to get all frames from a camera), then the other set can be used.

Decompression codecs.

Codecs are used for encoding and decoding video data

Description.

Here you can type a description of the camera shown to all users in the Spotter program.

Administrative Description.

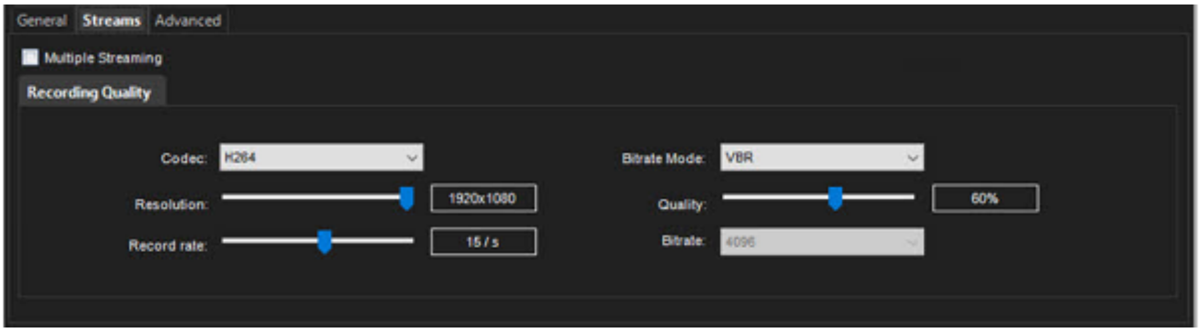
Here you can type a description of the camera. The description will be shown in the Spotter program to only system administrators.

Reference image

A reference image is an image captured from the camera, making it easier to identify the cameras. In addition, in the Spotter program, the users can compare what they see in the video view against the reference image to ensure that the camera is pointed in the right direction.
To change the current reference image, click the **Capture image** button. To delete a reference image, click the **Delete image** button.

Streams

By default, Mirasys VMS receives recording quality stream from the camera.
Mirasys VMS server send recording stream by default to the Mirasys Spotter.



□ Multiple Streaming

Codec: H264
Resolution: 1920x1080
Record rate: 15 / s
Bitrate Mode: VBR
Quality: 60%
Bitrate: 4096

Codec

The codec is used for transmitting the video between the server and the client applications, and in the case of IP cameras, for transmitting the video between the IP camera and the server.
In the case of analogue cameras, the codec used by the system is JPEG.
In IP cameras, any codec supported by both the camera and the server software can be selected.
The codecs supported by the server software are JPEG, MPEG-4, H.264, H.265 and Mobotix MxPEG.

Bitrate mode.

This setting controls if the Variable bit rate (VBRMax) or Constant bit rate (CBR) is used.

Quality

Set this value between 0%-100%. A higher value means better image quality but also a large image data size.

To decrease the image data size, set the value lower. However, setting the value lower also decreases the quality of the images.

50% is usually sufficient. For wireless and low bandwidth connections, select 0%.

Resolution

For automatically configured IP cameras, the exact image resolutions supported by the camera model are displayed.

Record rate

The record rate defines how many frames the camera sends to the VMS and how many frames are recorded.

The maximum rate depends on the video standard and the camera type.

Multiple streaming (multi-streaming)

Multi-Streaming

Multi-streaming enables separate feeds from a single camera.

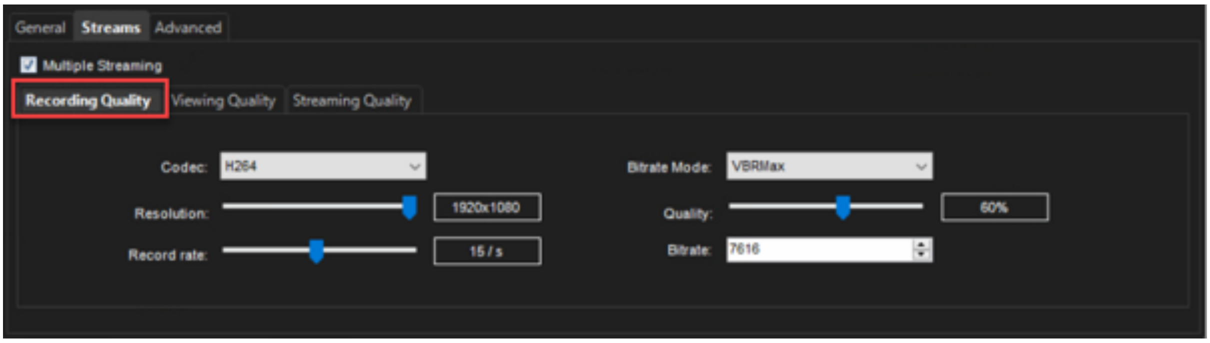
The feature allows for separate streams to be used for recording and viewing.

The feature is available only if the camera and driver support it.

Recording Quality

By default, Mirasys VMS receives recording quality stream from the camera.

Mirasys VMS server send recording stream by default to the Mirasys Spotter



☑ Multiple Streaming

Codec: H264

Resolution: 1920x1080

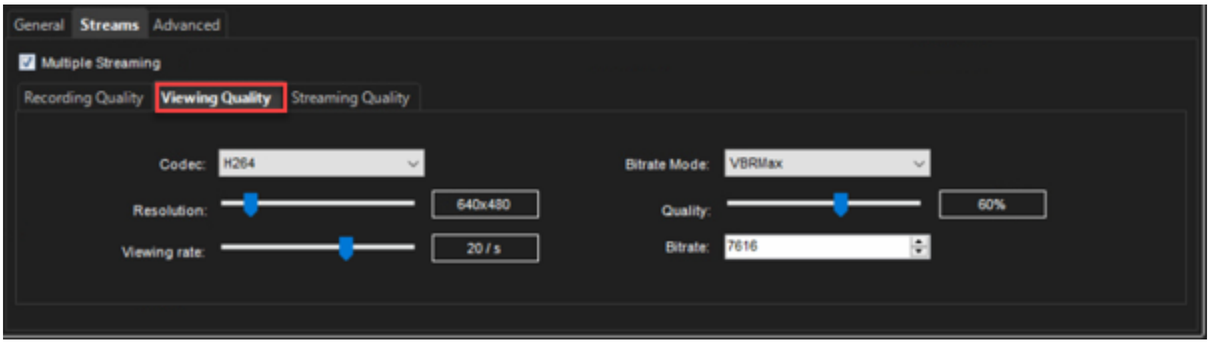
Record rate: 15 / s

Bitrate Mode: VBRMax

Quality: 60%

Bitrate: 7616

Viewing Quality



☑ Multiple Streaming

Codec: H264

Resolution: 640x480

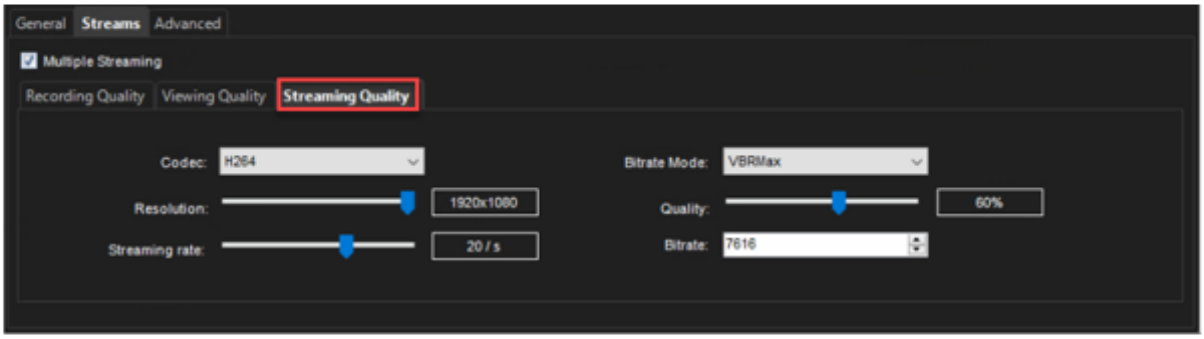
Viewing rate: 20 / s

Bitrate Mode: VBRMax

Quality: 60%

Bitrate: 7616

Streaming Quality



☑ Multiple Streaming

Codec: H264

Resolution: 1920x1080

Streaming rate: 20 / s

Bitrate Mode: VBRMax

Quality: 60%

Bitrate: 7616

Advanced

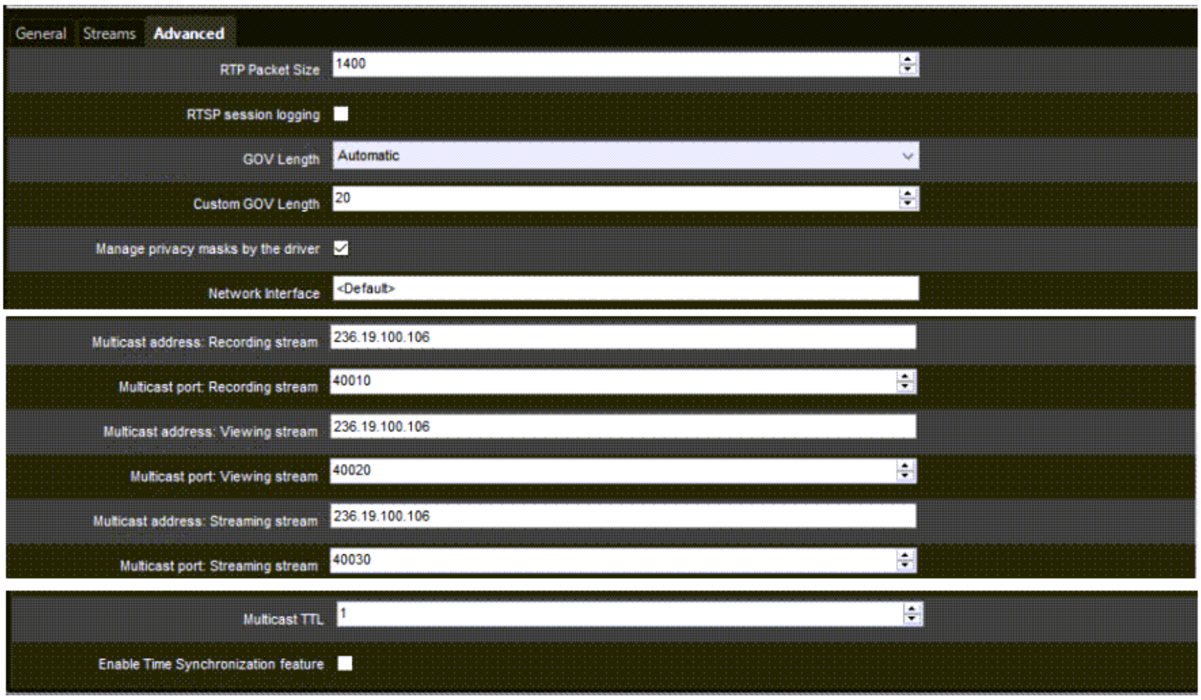
This tab contains camera or driver-specific unique settings. A driver update may bring additional values to this tab.

Selecting multiple cameras is possible with SHIFT or CTRL keys.

Please note that if you select more than one camera, you cannot set parameters not supported by all selected cameras.

Configurable values

1. RTP Packet Size
2. RTSP session logging
3. GOV Lenght
4. Custom GOV Lenght
5. Manage privacy mask by the driver
6. Network interface
7. Multicast address: Recording stream
8. Multicast port: Recording stream
9. Multicast address: Viewing stream
10. Multicast port: Viewing stream
11. Multicast address: Streaming stream
12. Multicast port: Streaming stream
13. Multicast TTL



RTP Packet Size	1400
RTSP session logging	□
GOV Length	Automatic
Custom GOV Length	20
Manage privacy masks by the driver	☑
Network Interface	<Default>
Multicast address: Recording stream	236.19.100.106
Multicast port: Recording stream	40010
Multicast address: Viewing stream	236.19.100.106
Multicast port: Viewing stream	40020
Multicast address: Streaming stream	236.19.100.106
Multicast port: Streaming stream	40030
Multicast TTL	1
Enable Time Synchronization feature	□

Frame rate optimization

The slider is intended to estimate load when using the server both as a recording server and a client workstation.

The default assumption for local/remote use is 50%.

If this limits the number of cameras or use of desired camera settings, the slider can be dragged towards 100% to add all desired cameras with desired settings.

However, care should be taken not to overload the server in such a situation.

After specifying whether frame rates should be optimized for local or remote viewing, click **Optimize.**The system sets the record rates to the highest possible values.

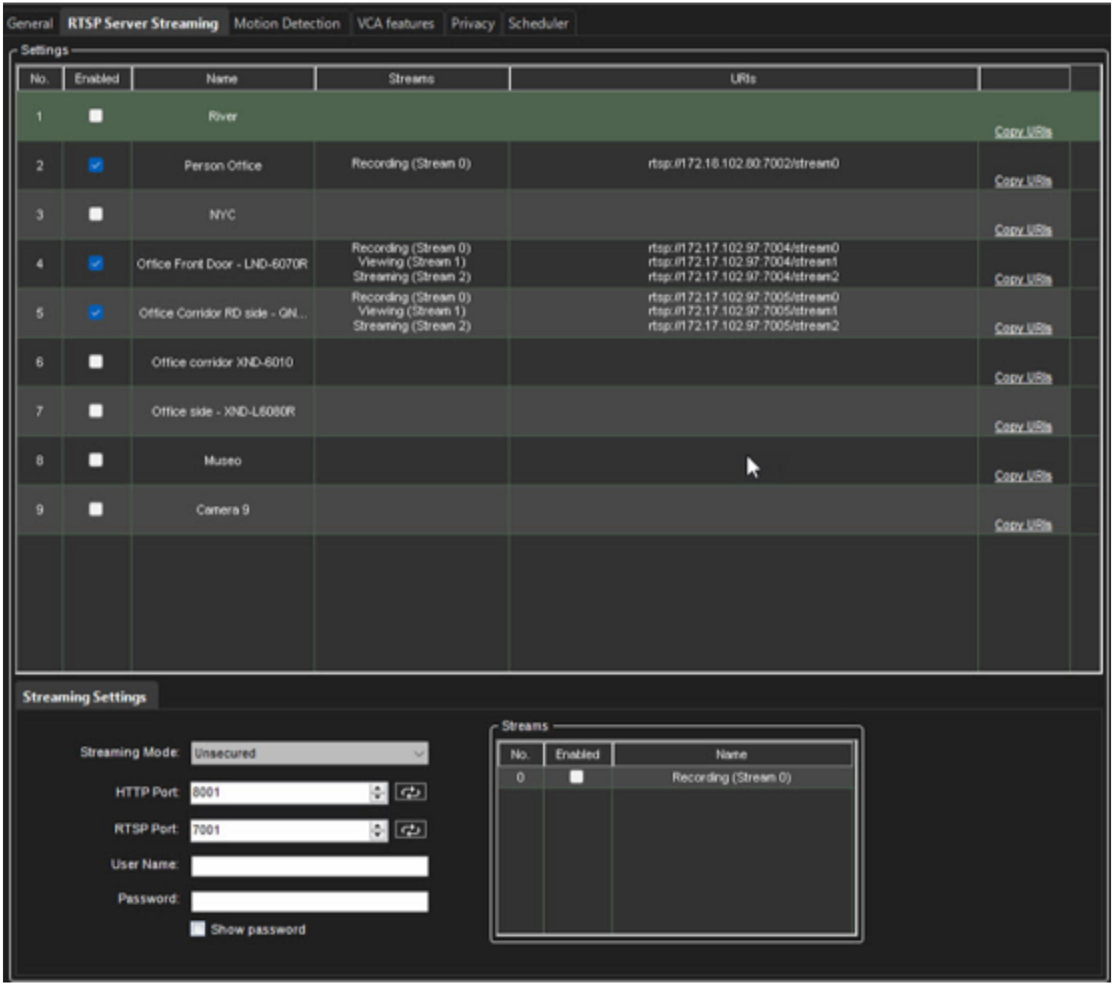
RTSP Server Streaming

Supported from V9.5

RTSP/RTSPS server is used to stream video from the server to any third-party client that supports RTSP/RTSPS protocol.

Settings

- Camera number
- Enabled/disabled check-box - allow user to enable/disable streams from specified camera without changing the settings
- Camera name
- List of configured streams
- List of configured stream URIs
- Copy URIs link - to copy to clipboard URIs for specified camera



Settings

No.	Enabled	Name	Streams	URIs	
1	□	River			Copy URIs
2	☑	Person Office	Recording (Stream 0)	rtsp://172.18.102.80:7002/stream0	Copy URIs
3	□	NYC			Copy URIs
4	☑	Office Front Door - LND-6070R	Recording (Stream 0) Viewing (Stream 1) Streaming (Stream 2)	rtsp://172.17.102.97:7004/stream0 rtsp://172.17.102.97:7004/stream1 rtsp://172.17.102.97:7004/stream2	Copy URIs
5	☑	Office Corridor RD side - QN...	Recording (Stream 0) Viewing (Stream 1) Streaming (Stream 2)	rtsp://172.17.102.97:7005/stream0 rtsp://172.17.102.97:7005/stream1 rtsp://172.17.102.97:7005/stream2	Copy URIs
6	□	Office corridor XND-6010			Copy URIs
7	□	Office side - XND-L6080R			Copy URIs
8	□	Museo			Copy URIs
9	□	Camera 9			Copy URIs

Streaming Settings

Streaming Mode: Unsecured

HTTP Port: 8001

RTSP Port: 7001

User Name:

Password:

□ Show password

Streams

No.	Enabled	Name
0	□	Recording (Stream 0)

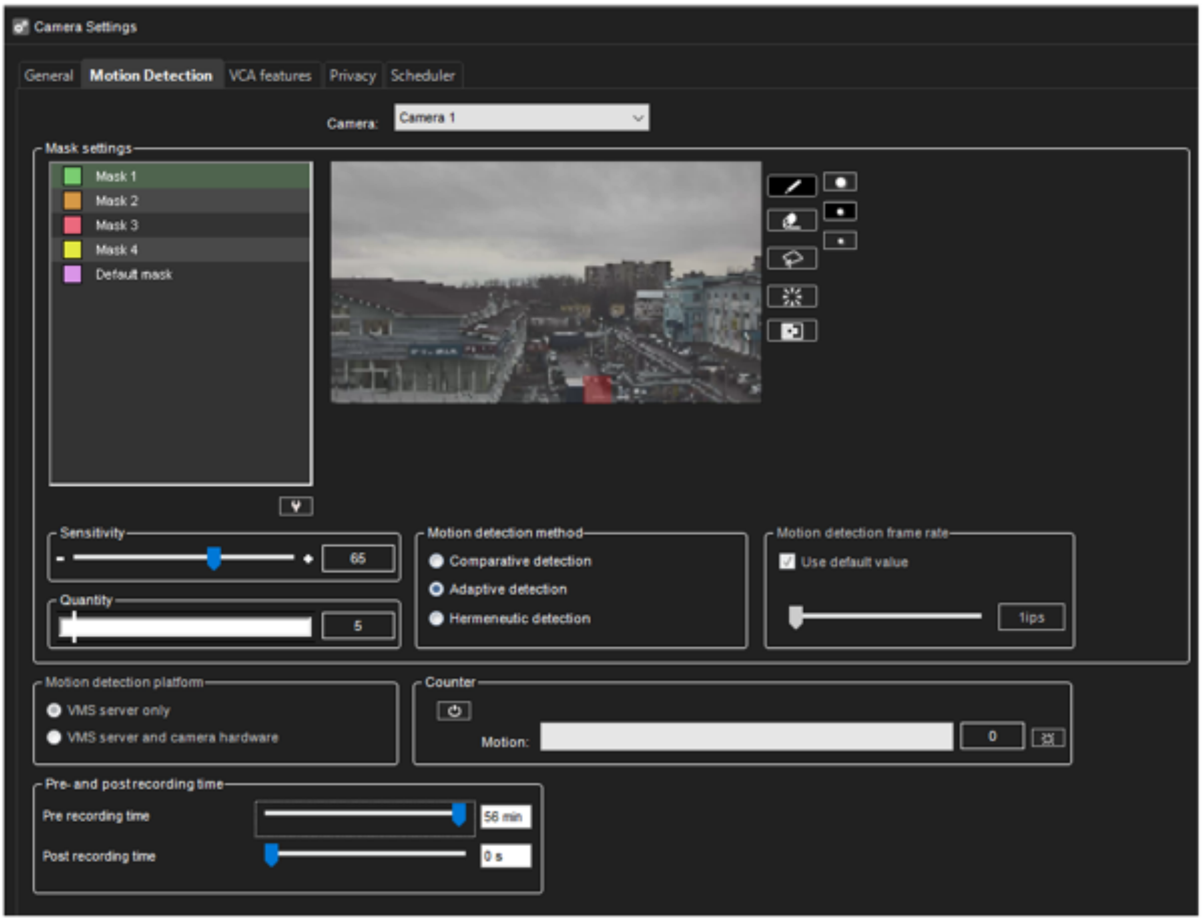
Streaming Settings

- Streaming mode - can be "Unsecured", Secured (UDP) and Secured (TCP). In secured mode instead of user name and password the certificate should be specified.
- HTTP Port - port for HTTP connection. Ports should be unique for each camera. User can use the "Test port" button to check if selected port is already used in recorder side.
- RTSP Port - port for RTSP connection. Ports should be unique for each camera. User can use the "Test port" button to check if selected port is already used in recorder side.
- Enabled/disabled check-box - allow user to enable/disable streams from specified camera without changing the settings
- User Name
- Password
- List of streams (multiple if multiple streaming is active) - each stream can be enabled/disabled separately

Enabling RTSP Server stream to the camera

1. Check the **Enabled** box from the selected camera
2. Select the line of the camera
3. Set **Streaming Mode**, **HTTP Port**, **RTSP Port**, **Username** and **Password**
4. Define used streams

Motion Detection



Camera Settings

General | Motion Detection | VCA features | Privacy | Scheduler

Camera: Camera 1

Mask settings
- 🟩 Mask 1
- 🟧 Mask 2
- 🟥 Mask 3
- 🟨 Mask 4
- 🟪 Default mask

Sensitivity: 65

Quantity: 5

Motion detection method
- ○ Comparative detection
- ● Adaptive detection
- ○ Hermeneutic detection

Motion detection frame rate
- ☑ Use default value
- 1ips

Motion detection platform
- ○ VMS server only
- ○ VMS server and camera hardware

Counter
- Motion: 0

Pre- and post recording time
- Pre recording time: 56 min
- Post recording time: 0 s

Sensitivity and quantity

The system detects motion when:

- Pixels change more than the set limit (**Sensitivity**).
- The specified number of pixels change (**Quantity**).

If there is a lot of background noise in the image, for example, changes in lighting conditions, decrease the sensitivity by dragging the slider to the left or increase the quantity limit by dragging the slider to the right.

Motion detection methods

Comparative detection

Compares an image to the image before it. If the differences exceed the set limits, the system detects motion.

You can use comparative motion detection in most conditions.

However, if there is a lot of movement in the background, for example, rain, moving leaves, or changes in light levels, use adaptive motion detection.

Adaptive detection

Compares each image to a background image. The system learns the background image and the movement that belongs there automatically.

Thus, the system does not interpret, for example, moving leaves as motion.

In addition, if more than half of the pixels in an image change, the system concludes that the lighting conditions have changed.

As a result, it resets the reference image and starts learning it again.

Hermeneutic detection

Is a sophisticated motion detection system for challenging weather conditions (e.g. heavy rain, “noisy” background image, etc.) and situations in which external video content analytics (VCA) tools are used.

It should be noted that hermeneutic detection requires more processing resources than the other detection methods.

Motion detection frame rate

Defines the frame rate used in motion detection.

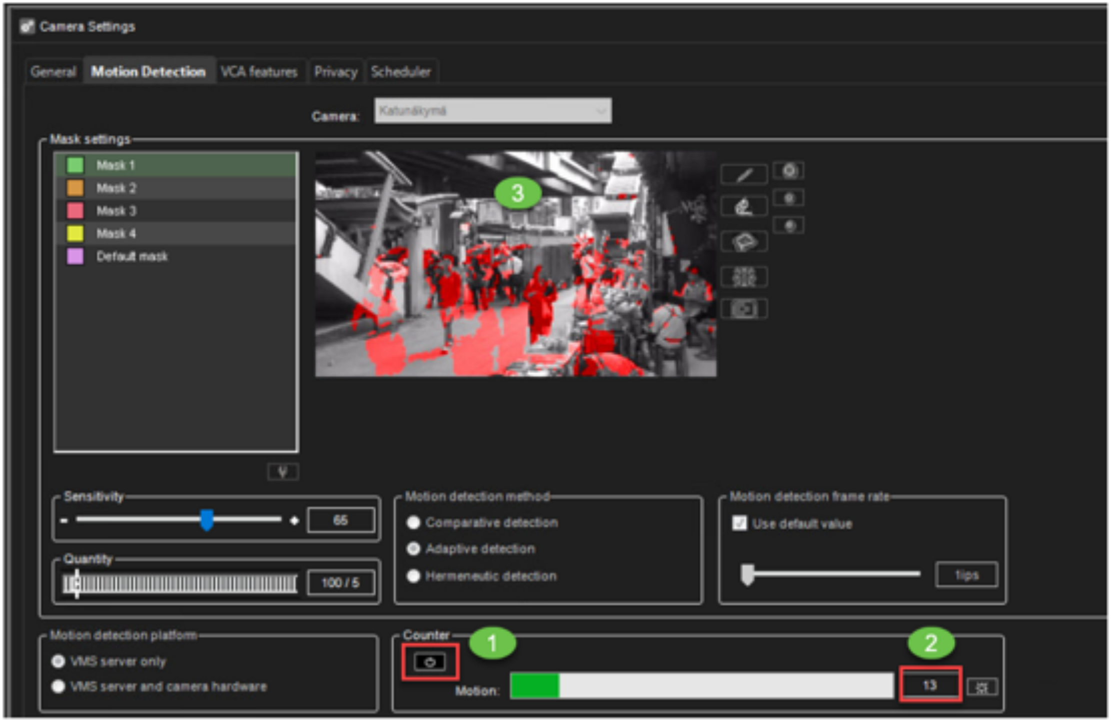
It is generally recommended to use the default frame rate.

For IP cameras, motion detection uses intra-frames and matches the intra-frame rate.

Typically, this is one image per second.

Counter

1. Enable **Counter**
2. Check the motion values
3. The camera image shows which area of the camera image causes motion detection recording



Camera Settings

General | Motion Detection | VCA features | Privacy | Scheduler

Camera: Katunäkymä

Mask settings
- 🟩 Mask 1
- 🟧 Mask 2
- 🟥 Mask 3
- 🟨 Mask 4
- 🟪 Default mask

Sensitivity: 65

Quantity: 100 / 5

Motion detection method
- ○ Comparative detection
- ● Adaptive detection
- ○ Hermeneutic detection

Motion detection frame rate
- ☑ Use default value
- 1ips

Motion detection platform
- ● VMS server only
- ○ VMS server and camera hardware

Counter

Motion: 13

Pre- and Post- recording time

Supported from V9.5

Motion pre-and post-recording is used to have recorded material before and after the motion.

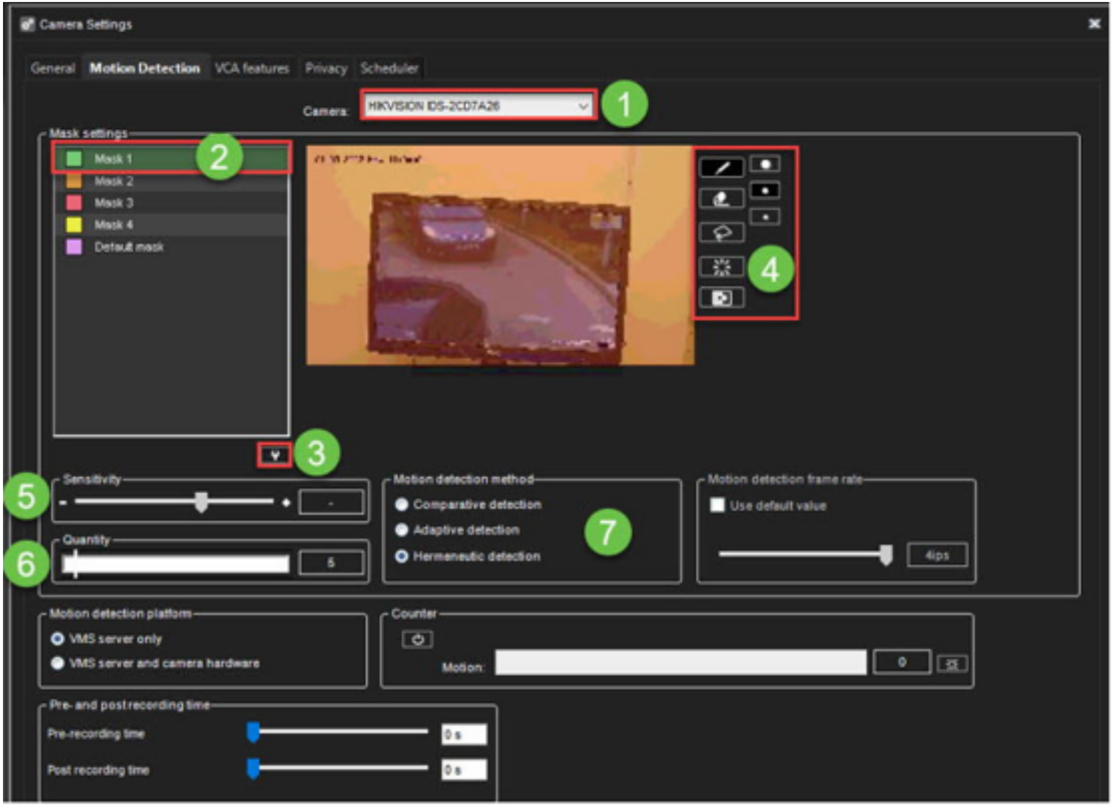
Each mask can be configured separately.

Values are from 0s to 60 minutes.

The user can copy selected values to the all cameras using button **Copy pre-and post recording time for all cameras.**

Editing a mask

1. In the **Motion Detection** tab, select the camera from the camera list.
2. Click the mask that you want to edit.
3. To change the mask's name, click **Change Mask Name** and type a new name for the mask.



Camera Settings

Camera: HIKVISION DS-2CD7A26

Mask settings: 🟩 Mask 1, Mask 2, Mask 3, Mask 4, Default mask

Sensitivity: -

Quantity: 5

Motion detection method: ○ Comparative detection ○ Adaptive detection ● Hermeneutic detection

Motion detection frame rate: □ Use default value 4fps

Motion detection platform: ● VMS server only ○ VMS server and camera hardware

Counter: Motion: 0

Pre- and post recording time: Pre-recording time 0 s; Post recording time 0 s

1. With the drawing tools presented in the following table, paint the areas red where you want the system to detect movement and remove the red from areas where you want to ignore the movement.
2. Set the detection sensitivity.
3. Set the minimum quantity of movement.
4. Select the motion detection method: comparative, adaptive, or hermeneutic motion detection.

Detected motion is shown in red in the image, and the counter increments each time motion is detected.

Drawing Tools:

Tool	Name	Description
	Pencil	Use to set the motion detection area. Select the pencil size by clicking one of the tool size buttons (large, medium, small).
	Eraser	Use to erase selected areas that you do not want to include. Select the eraser size by clicking one of the tool size buttons (large, medium, small).
	Lasso	Use to select areas using straight lines. If the pen tool is selected, using this tool adds to selected areas. If the eraser tool is selected, this tool removes from the selection. Click the image where you want to start the selection. Click again where you want to anchor the line and change direction. To complete the selection, click the starting point. The selected area is painted red, or the red colour is removed.
	Fill/Clear	If the pen tool is selected, clicking this button selects the total image area. If the eraser tool is selected, clicking this button removes all selections.
	Invert	Reverses selected and unselected areas. Sometimes it is easier to select the area you do not want to mask and then invert the selection.

●	Tool Size	Click one of the buttons to select the size of the pencil or eraser (large, medium, small).

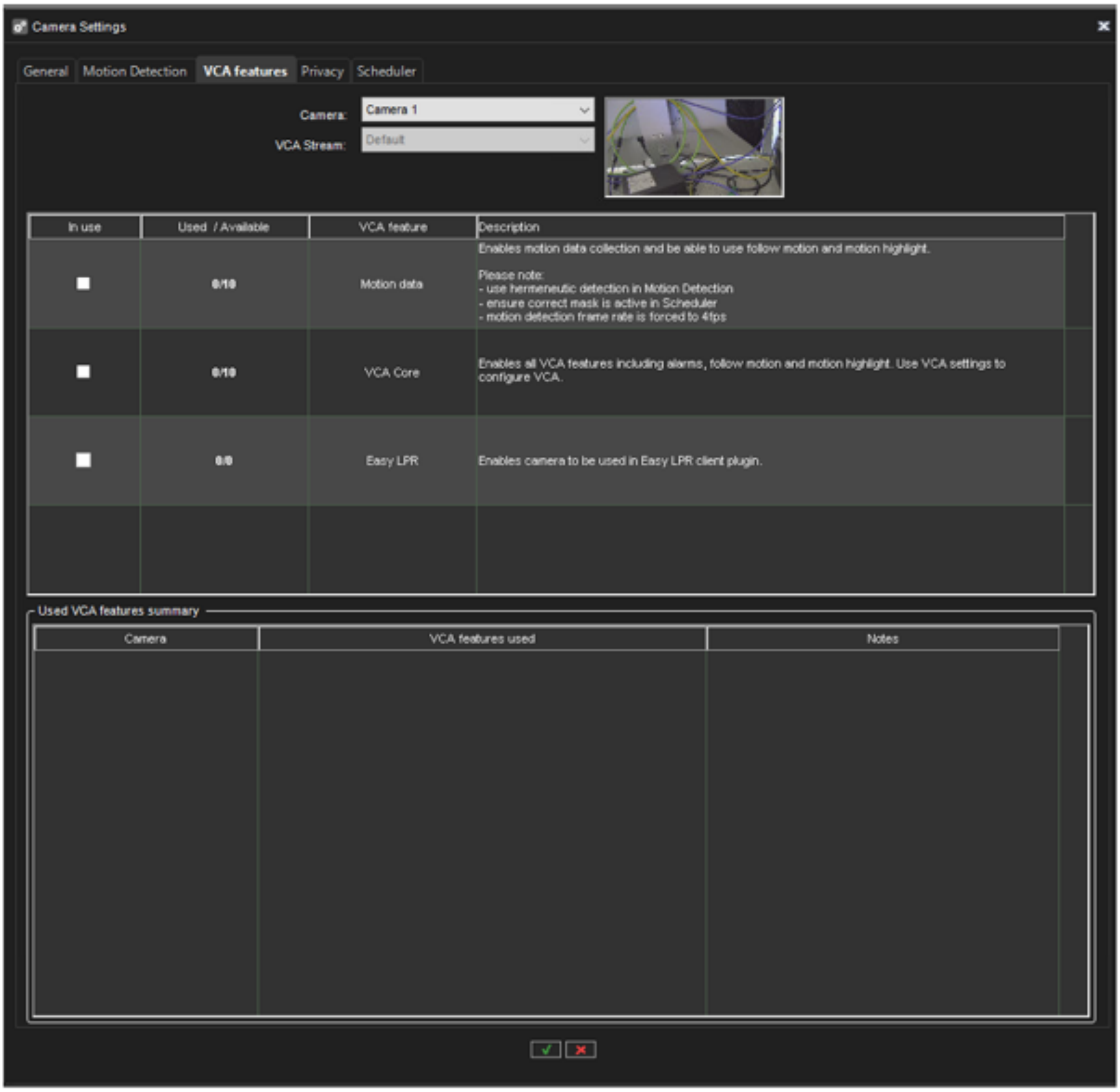
VCA features

If the software license includes Video Content Analytics (VCA) functionality, it can be administered on a camera-specific basis on the **VCA Features** -tab.

Depending on the license, specific VCA functionalities can be enabled or disabled on the tab.

It is possible to control which stream (in a configured camera to use multiple streaming) is used for VCA.

This is achieved from the pull-down menu below the camera selector (see the following mage)



Camera: Camera 1

VCA Stream: Default

In use	Used / Available	VCA feature	Description
□	0/10	Motion data	Enables motion data collection and be able to use follow motion and motion highlight. Please note: - use hermeneutic detection in Motion Detection - ensure correct mask is active in Scheduler - motion detection frame rate is forced to 4fps
□	0/10	VCA Core	Enables all VCA features including alarms, follow motion and motion highlight. Use VCA settings to configure VCA.
□	0/0	Easy LPR	Enables camera to be used in Easy LPR client plugin.

Used VCA features summary

Camera	VCA features used	Notes

Figure 12 The VCA Features tab

In the primary state, the tab contains the following VCA features:

- **Motion data:** Internal VCA motion data, enabling data collection, motion following, and motion highlighting. Visualized in **Mirasys Spotter**.

- **VCA Core:** enables full VCA functionality. Configured through VCA settings in system manager.
- **Easy LPR**: Enables the camera to be used in the Easy LPR Client plugin

Please note that the VCA features are only available if enabled through the license.

Privacy

Under the Privacy menu, you can control the privacy zones of the camera and the facial- and movement blurring functionality.

To be noted: the content of the privacy functionalities is available (for the user) only if they are defined for the camera.

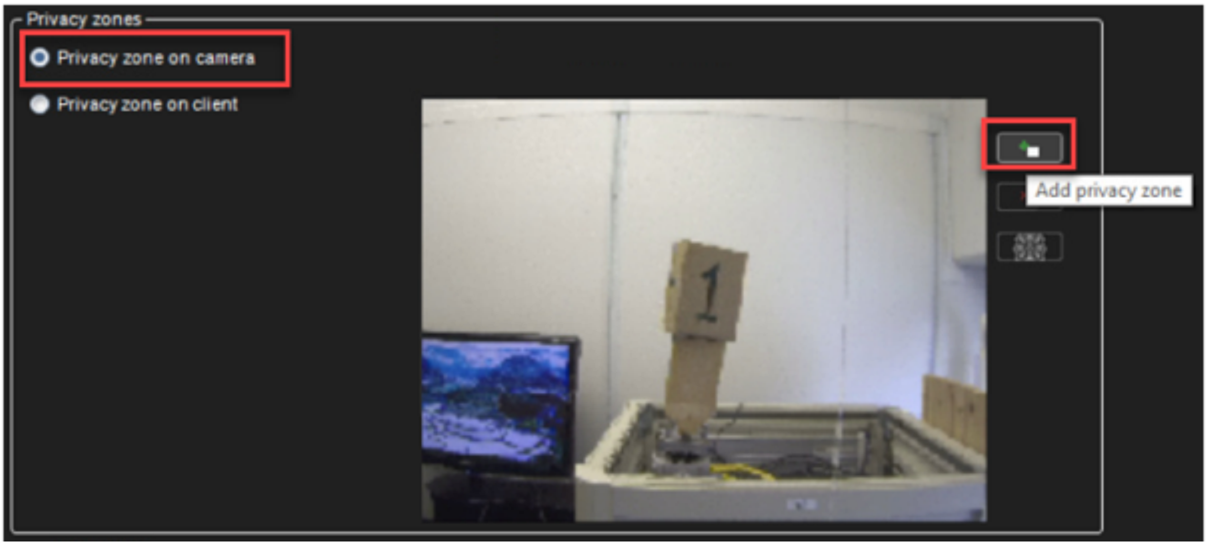
(I.e. if the camera does not have, e.g. the facial blurring defined, this camera shall not have the faces blurred – even if the user group of the end-user would have permission level set to view only unblurred materials.

This also applies when exporting the materials.

Privacy zone on the camera

Adding privacy zone

1. In the **Privacy Zones** tab, select the camera from the camera list.
2. Select **Privacy zone on the camera**
3. Click **Add privacy zone**.
4. Paint the privacy zone onto the camera view. The newly created zone is displayed in semi-transparent light grey. You can resize and move the zone by dragging it.
5. Repeat steps 1-3 to create as many private zones as required.
6. Click **OK**.



Removing the privacy zone

To remove privacy zones:

1. In the **Privacy Zones** tab, select the camera from the camera list.
2. Click on a privacy zone in the camera view.
3. Click **Remove privacy zone** or **Remove all privacy zones**.
4. Click **OK**.

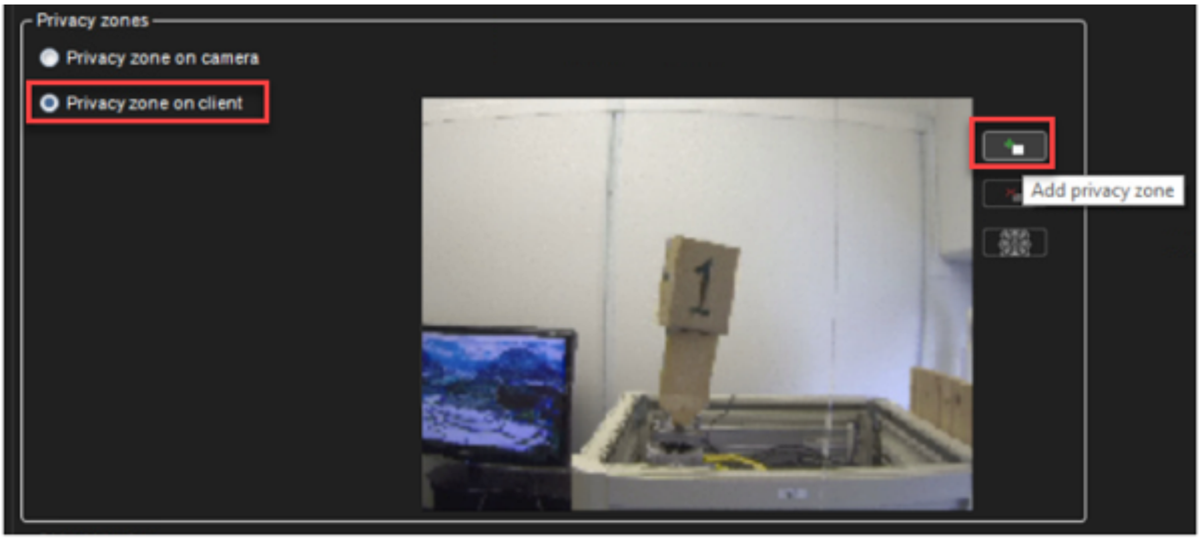
Privacy zone on the client

On the Spotter client: these privacy zones are implemented only on the viewing client.

This allows the complete video to be recorded and exported, but the privacy-screened areas are only accessible for users who have the right to do so.

Adding privacy zone

1. In the **Privacy Zones** tab, select the camera from the camera list.
2. Select **Privacy zone on the client**
3. Click **Add privacy zone**.
4. Paint the privacy zone onto the camera view. The newly created zone is displayed in semi-transparent light grey. You can resize and move the zone by dragging it.
5. Repeat steps 1-3 to create as many private zones as required.
6. Click **OK**.



Removing the privacy zone

To remove privacy zones:

1. In the **Privacy Zones** tab, select the camera from the camera list.
2. Click on a privacy zone in the camera view.
3. Click **Remove privacy zone** or **Remove all privacy zones**.
4. Click **OK**.

Object Blurring

“Blur faces” and “Blur moving objects” settings are available to be set up as additional privacy.

If the facial- or motion-based blurring is enabled for a camera, these are also available on the Spotter side (provided that the user has sufficient permissions.)

The blurring will not be functional on the spotter side- or for exports of the video material for the cameras if they have not been selected on the system administrator side.

Higher resolutions used for the algorithms mean higher accuracy for the algorithms- but also higher CPU loads.

Blur Faces

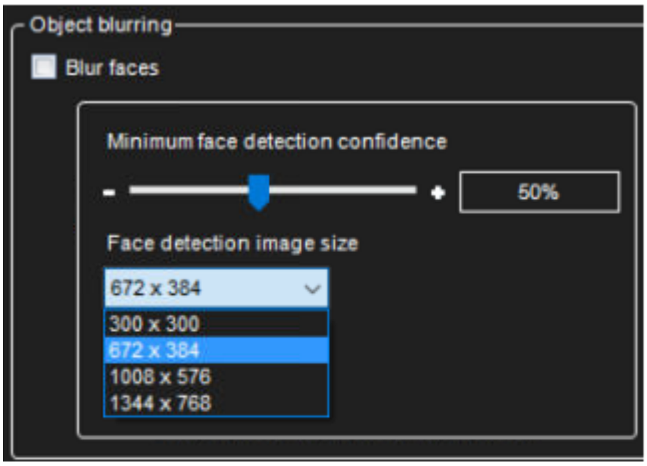
Minimum face detection confidence

Face detection image size

Using a small face detection size value, a person face must be closer to the camera. Face detection will be faster.

Using bigger face detection size value. a person's face is detected more away from the camera.

1. 300x384
2. 672x384
3. 1008*576
4. 1344x768



Object blurring

□ Blur faces

Minimum face detection confidence: 50%

Face detection image size: 672 x 384

Blur Moving objects

Motion detection sensitivity

How sensitively pixel in the image is detected as motion pixel

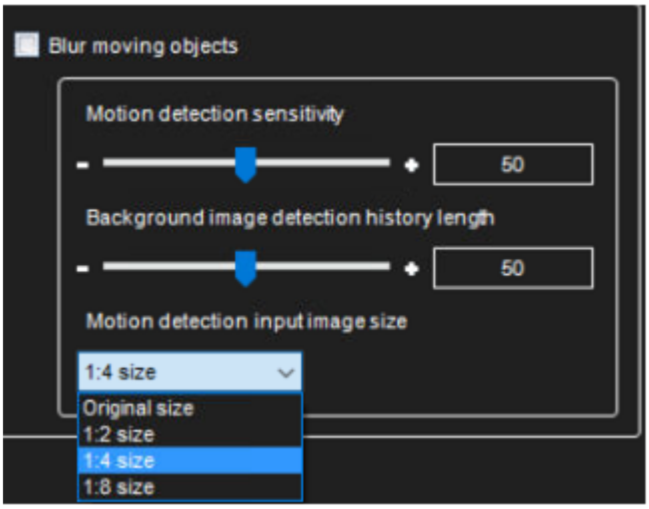
Background image detection history length

How quickly stationary objects are detected as background

Motion detection input image size

The smaller size is quicker to process but outputs the worse results.

1. Original size
2. 1:2 size
3. 1:4 size
4. 1:8 size



□ Blur moving objects

Motion detection sensitivity: 50

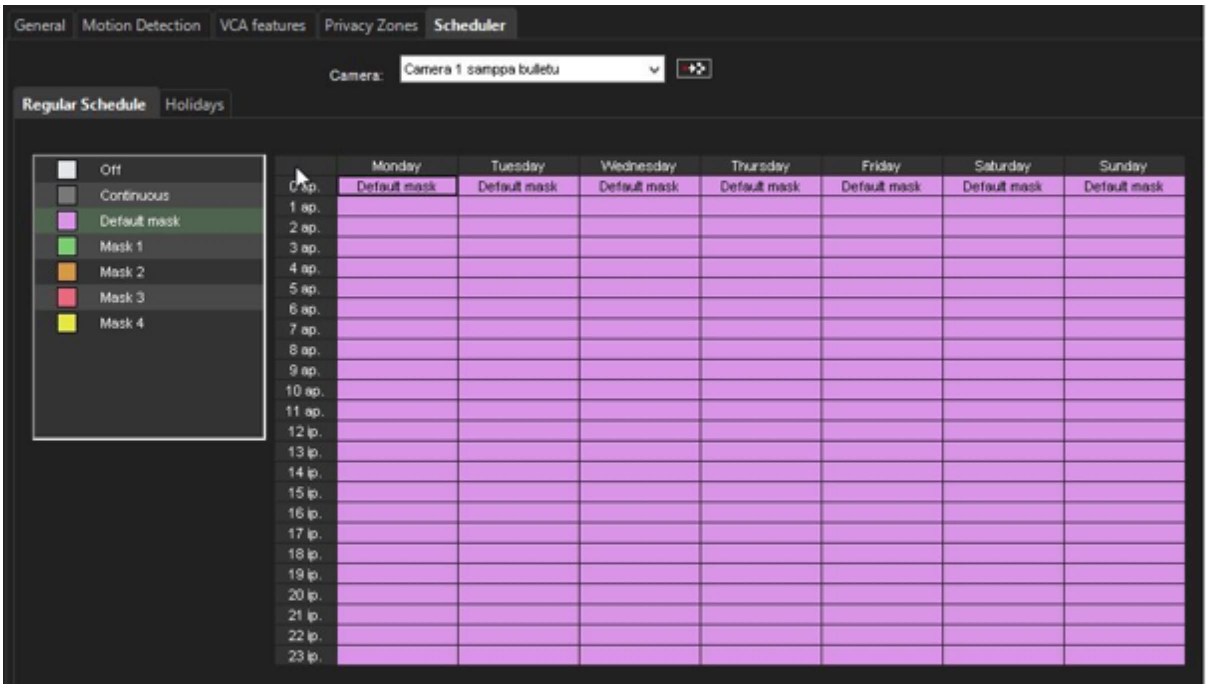
Background image detection history length: 50

Motion detection input image size: 1:4 size

Scheduler

Scheduler defines which mask is used on each camera and what is active days and hours for the mask.

By default, video is recorded when the system detects motion in the default mask. The default mask is active 24/7.



Camera: Camera 1 samppa bulletu

⬜ Off
▨ Continuous
🟪 Default mask
🟩 Mask 1
🟧 Mask 2
🟥 Mask 3
🟨 Mask 4

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
0 ap.	Default mask	Default mask	Default mask	Default mask	Default mask	Default mask	Default mask
1 ap.							
2 ap.							
3 ap.							
4 ap.							
5 ap.							
6 ap.							
7 ap.							
8 ap.							
9 ap.							
10 ap.							
11 ap.							
12 ip.							
13 ip.							
14 ip.							
15 ip.							
16 ip.							
17 ip.							
18 ip.							
19 ip.							
20 ip.							
21 ip.							
22 ip.							
23 ip.							

However, you can set different options for each hour of the week. For example, use different motion detection masks during the day and the night.

First, set the regular weekly schedule on the **Regular Schedule** tab and then, if necessary, set holiday schedules on the **Holidays** tab.

To change the schedule, click on the mask you want to activate, and then click on the scheduled hour where you want it to be used.

Tip: *To change more than one hour at the same time, drag with the mouse.*

You can also click the first cell, keep the SHIFT key pressed and then click the last http://cell*. To change all hours in a column or a row, click the column or row heading. To change all hours of the week, click the cell above the hour's column (on the left side of the weekday heading row).*

These options are available:

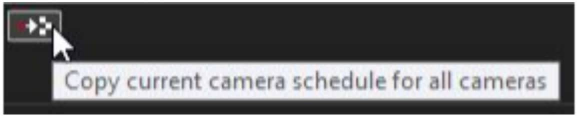
1. **Off**. Video is not recorded. However, possible alarms are recorded. Alarms are configured in **Alarm Settings**.
2. **Continuous.** The camera records all images. This option uses a lot of disk space.

3. **Default mask.** The camera records video using the default motion detection mask and default motion detection parameters.
4. **Custom mask.** The camera records video using a custom mask. Each camera can have as many as four custom masks.

To copy the current schedule for all cameras:

You can copy the currently selected recording schedule for all cameras in the system.

1. Click Copy Schedule .



2. When asked for confirmation, click **OK**.

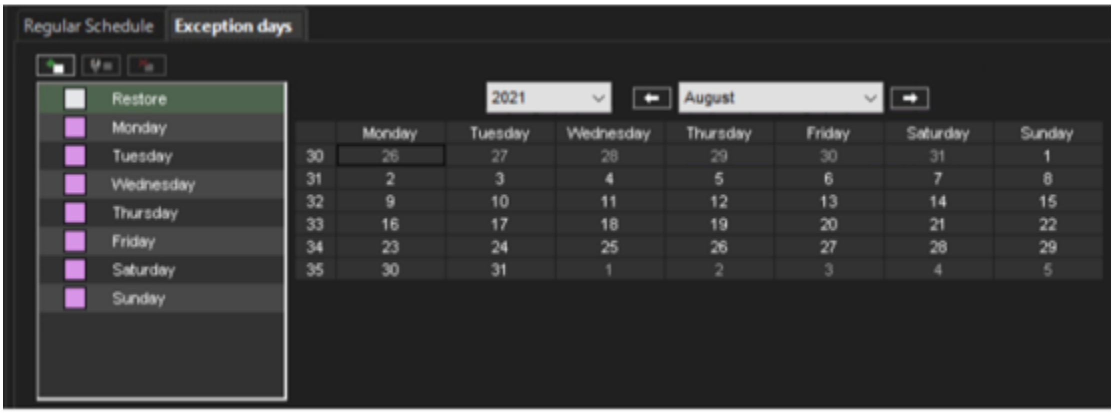
An exception days settings allow you to set holidays to the calendar.

To set an exception day schedule:

You can use different recording schedules for holidays.

You can apply a daily schedule from the **Regular Schedule** or use an **Exception days** schedule.

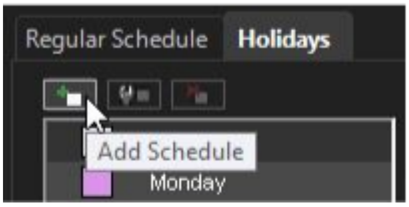
1. On the **Exceptions days** tab, select the year and month.
2. Click the schedule that you want to apply from the left panel and then click the holiday in the calendar.



	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
30	26	27	28	29	30	31	1
31	2	3	4	5	6	7	8
32	9	10	11	12	13	14	15
33	16	17	18	19	20	21	22
34	23	24	25	26	27	28	29
35	30	31	1	2	3	4	5

To add a custom schedule:

Click **Add Schedule**



1. Type a name for the schedule.
2. Click the mask you want to apply and then click the hours you want to apply the mask to.
3. Click **OK**.

To edit a custom schedule:

1. Select the schedule and click **Edit Schedule**.
2. Edit the schedule and click **OK**.

To delete a custom schedule:

- Select the schedule from the left pane and click **Delete Schedule**.

To restore the original schedule:

Click **Restore** and then click the day that you want to restore.

License Plate Recognition settings

> The **Smart LPR** feature requires an **RTSP Server Streaming** license.

Configuration

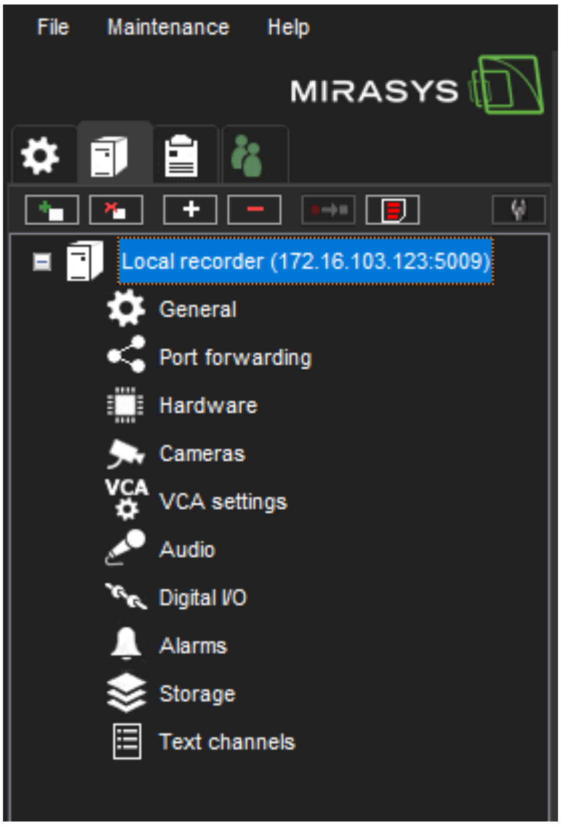
How to configure License Plate Recognition (LPR) services via System Manager:

Open the System Manager application. The LPR settings and settings' limits start loading during the open application after inputting the login and password.

If your license does not support the **Smart LPR** feature, the **LPR settings** tab will be hidden.

Change or set LPR settings

1. To change or set LPR settings, select recorder on the **VMS servers** tab and open the tree node:



2. Double-click the item “Cameras” to open the **Camera Settings** window

3. Click on the **LPR settings** tab to manage LPR settings.

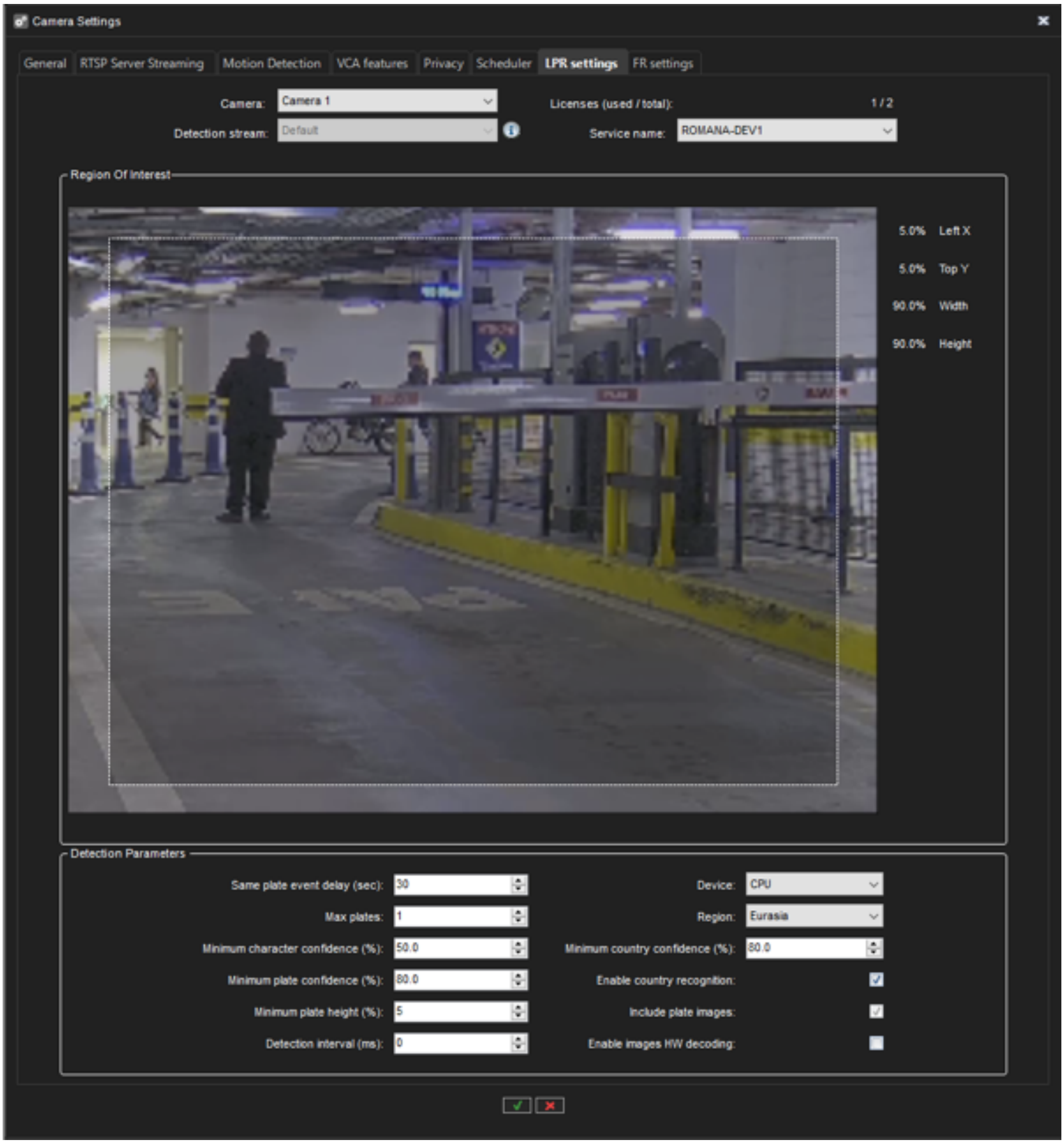
Please note when you double-click the item **Cameras** in the open **Camera Settings** window, your license checks for the ability to use the **Smart LPR** feature and generates a list of cameras (for Combobox **Camera** on the **LPR settings** tab) that are used or can be used in the LPR services.

4. When you select the **LPR settings** tab, the first camera from the Combobox **Camera** is selected.

If the selected camera can be found in services settings, the settings of this service are loaded.

Above the **Service name** Combobox, you will find the **Licenses (used / total)** Label with the number of currently used LPR licenses and total LPR licenses. When you choose a service for a camera and stream current license count is increased, and if you choose a “None” service for a camera, then the current license count is decreased.

*Note: a stream is started in the **Region Of Interest** group area immediately after the current camera is selected in the **Camera** Combobox.*



Camera: Camera 1

Detection stream: Default

Licenses (used / total): 1 / 2

Service name: ROMANA-DEV1

5.0% Left X

5.0% Top Y

90.0% Width

90.0% Height

Same plate event delay (sec): 30

Max plates: 1

Minimum character confidence (%): 50.0

Minimum plate confidence (%): 80.0

Minimum plate height (%): 5

Detection interval (ms): 0

Device: CPU

Region: Eurasia

Minimum country confidence (%): 80.0

Enable country recognition: ☑

Include plate images: ☑

Enable images HW decoding: □

If no LPR service contains settings for this camera, then the “None” value is selected in the Combobox **Service name**, and the LPR settings are disabled.

You cannot enter service settings if RTSP streaming is not enabled for the selected camera and the stream on the **RTSP Server Streaming** tab. In this case **RTSP streaming should be enabled for selected camera and stream for change the license plate recognition settings** will appear instead of group boxes with LPR settings' controls

If the selected camera is used in some LPR service but is not allowed by the current LPR license for this service, then the **Selected camera for the current service is not allowed by the license. Release LPR service for this camera or for any other camera to keep the license for this one** comment will appear.

In such a case, switching the service name to the “None” value for the free license is possible.

If you need to keep the selected camera in the services settings, then should be a free license for the other camera. You need to select the other camera and switch the service name to the “None” value.

When configured licenses number equals total licenses number it is not possible to switch the service name for cameras with “None” service name value. In this case, **Service name** field will be disable for such cameras.

If the camera supports **ANPR**, you can select “Camera Engine” service in the **Service name** Combobox for such a camera. It means that all events created by the camera itself will be handled by the List Management service as normal **LPR** events.

When the “Camera Engine” service is selected, **Settings for Camera Engine are configured on the camera itself** will appear instead of group boxes with LPR settings' controls because, in this case, it is possible to change ANPR settings on the camera side only.

"License (used / total)" field shows how many licenses are used by LPR services and how many licenses are available. If license is unlimited "Unlimited" value is shown in this field.

Plate detection settings

After the camera, its stream and the LPR detection service are selected, license plate detection settings can be adjusted. Plate detection settings can be found in the **Detection Parameters** group box in the **LPR settings** tab in the **Camera Settings** window.

Plate detection settings are used for configuring the plate recognition detector.

- **Region of interest** - define the area where the detections are made.
- **Same plate event delay** - the number of seconds that should elapse before reading the same plate twice.
- **Max plates** - maximum number of plates to detect. Detected plates are sorted by plate confidence number in descending order.
- **Minimum character confidence** - plate characters recognizer confidence level. Valid values are between 25% - 95%.
- **Minimum plate confidence** - recognizer confidence level. Valid values are in the range of 25% - 95%.
- **Minimum plate height** - minimum plate height in %. Valid values are in the range 1% - 50%. The default value is 5%.
- **Detection interval** - the number of milliseconds that describes how often plate detection is done: if it is, for example, 250ms, then plate detection is done 4 times in a second (even if the video stream frame rate is much higher, like 30 fps).
- **Device** - is used for inference. Available devices depend on the hardware of the actual service.
- **Region** - The detection model (Eurasia or Americas) to be used for detection.
- **Minimum country confidence** - country recognizer confidence level. Valid values are between 25% - 95%.
- **Enable country recognition** - enable or disable country detection. Enabling country detection can improve plate number detection in some cases.
- **Include plate images** - include plate images or not in returned data.
- **Enable images HW decoding** - enable to decode input images with the most suitable computing platform (CUDA, DXVA, or DirectX).

Save settings

Click the **OK** button with the green checkmark icon at the bottom of the **Camera Settings** window.

Click the **Cancel** button with the red cross icon to cancel saving LPR settings and return to the settings values loaded after opening the **System Manager** application.

LPR settings for the selected camera are temporarily saved after switching on other cameras, streams, or tabs.

If you need to delete stream settings for the selected camera and detection stream, then select “None” in the **Service name** Combobx for the selected camera and detection stream.

Influence on settings

The following actions affect the service settings regardless of the actions on the **LPR settings** tab:

- *Deleting a recorder:* in case of deleting a recorder, all streams are deleted in the settings of all LPR services that worked with the remote recorder and saving the LPR settings.
- *Deleting a camera:* in case of deleting a camera, the stream is deleted in the settings of all LPR services that worked with this camera and saving LPR settings. There is a rule - one camera with one stream can only be used by one LPR service, but one LPR service can work with multiple cameras.
- *Changing the image size and compression type on the **Streams** subtab of the **General** tab:* in case of changing the resolution or compression type for the camera and stream, which are present in the settings of any LPR service, the LPR service settings are changed and saved when the **Camera Settings** window is closed.
- *Changing the RTSP streaming settings in the **Streaming Settings** group of the **RTSP Server Streaming** tab:* in case of changing the "Password,” “User Name“, "RTSP Port", "Streaming Mode" (security type) for the selected camera and stream, which are present in the settings of any LPR service, the LPR service settings are changed and saved when the **Camera Settings** window is closed.
- *Changing the image size in the **Device Settings** group of the **Video** tab in the **Hardware Settings** window:* in case of changing the resolution for the selected camera (here is possible to change the resolution for ***Recording*** stream only), which is present in the settings of any LPR service, the LPR service settings are changed and saved when the **Hardware Settings** window is closed.

- *Changing the camera by clicking on the **Edit IP camera** button on the **Video** tab in the **Hardware Settings** window:* in case of changing the camera by clicking on the ***Edit IP camera*** *button* resolution and compression type for the new camera (for ***Recording*** stream only) will be rewritten in LPR services settings, where camera ID is presented, the LPR service settings are changed and saved when the **Hardware Settings** window is closed.

Face Recognition Settings

How to configure Face Recognition (FR) Services in the System Manager.

Open the System Manager application. The FR settings and settings' limits start loading during the open application after inputting the login and password.

> If your license does not support the **Smart FR** feature, the **FR settings** tab will be hidden.

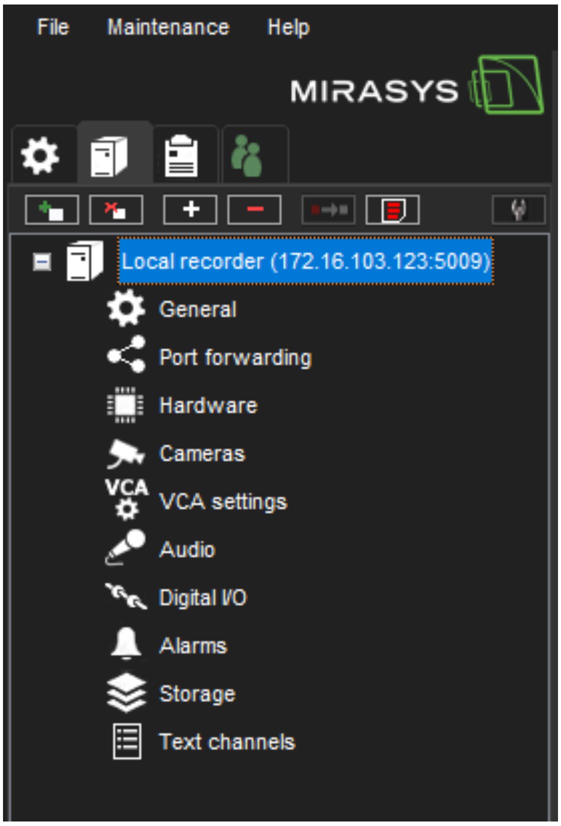
> The feature requires an **RTSP Server Streaming** license.

> Note that anti-spoofing is **not** included in version 9.6.

Open settings

- To change or set FR settings, select recorder on the

VMS servers tab and open the tree node:



2. Double-click the item “Cameras” to open the **Camera Settings** window:

3. Click the **FR settings** tab to manage FR settings.

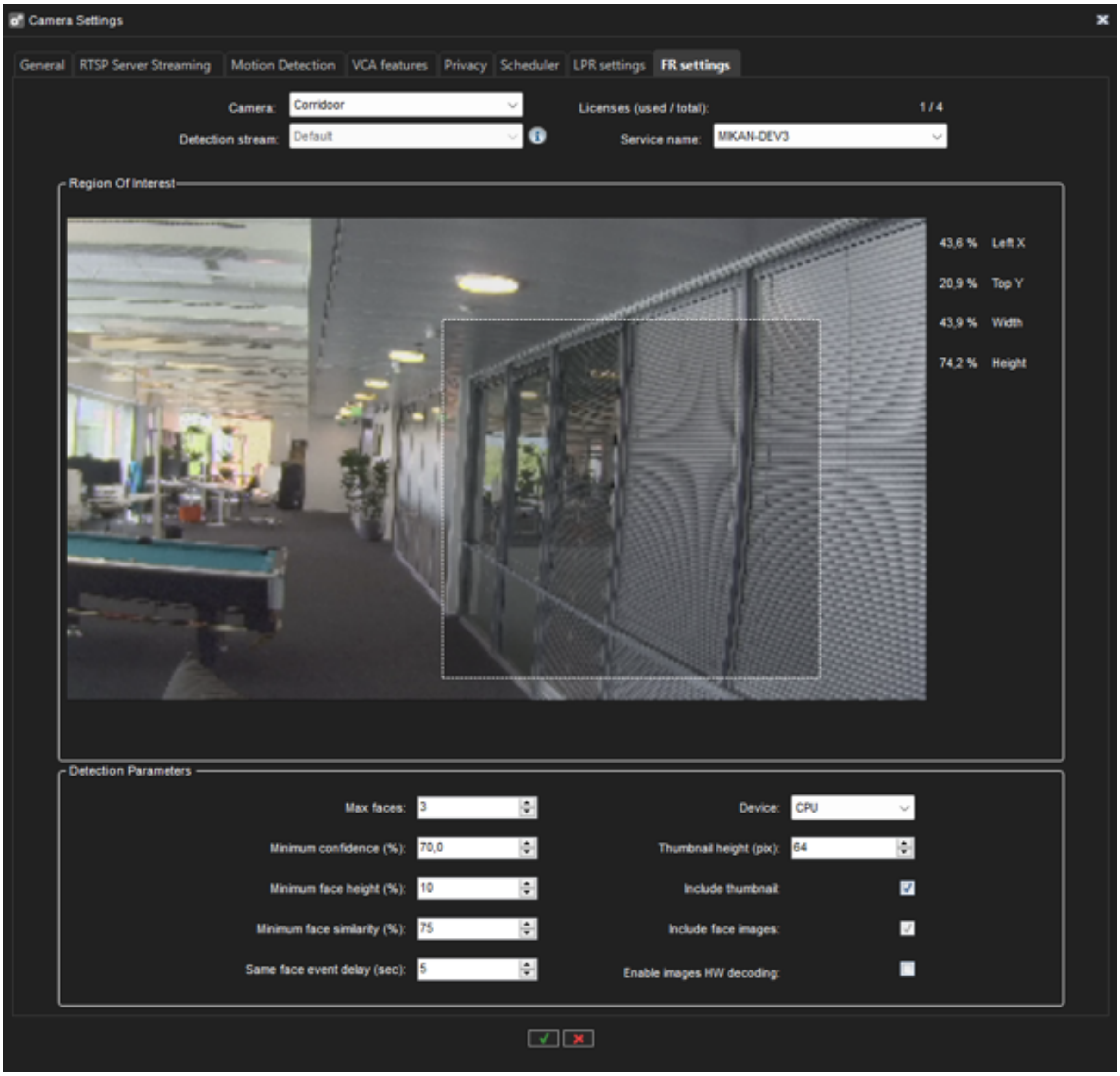
Please note that when double-clicking the item **Cameras** in the open **Camera Settings** window, the user license checks for the ability to use the **Smart FR** feature and generates a list of cameras (for Combobox **Camera** on the **FR settings** tab) that are used or can be used in FR services.

4. When selecting the **FR settings** tab, the first camera from the Combobox **Camera** is selected.

If the selected camera can be found in services settings, the settings of this service are loaded.

Above the **Service name** Combobox, you will find the **Licenses (used / total)** Label with the number of currently used FR licenses and total FR licenses. When you choose a service for a camera and stream current license count is increased, and if you choose a "None" service for a camera, then the current license count is decreased.

*Note: a video stream in the **Region Of Interest** group area is started immediately after the current camera is selected in the **Camera** Combobox.*



Camera: Corridoor

Detection stream: Default

Licenses (used / total): 1 / 4

Service name: MIKAN-DEV3

Region Of Interest

43,6 % Left X

20,9 % Top Y

43,9 % Width

74,2 % Height

Detection Parameters

Max faces: 3

Minimum confidence (%): 70,0

Minimum face height (%): 10

Minimum face similarity (%): 75

Same face event delay (sec): 5

Device: CPU

Thumbnail height (pix): 64

Include thumbnail: ☑

Include face images: ☑

Enable images HW decoding: □

If no FR service contains settings for this camera, then the "**None**" value is selected in the Combobox **Service name**, and the FR settings are disabled.

You cannot access service settings if RTSP streaming is not enabled for the selected camera and streams on the **RTSP Server Streaming** tab. Enable the **RTSP streaming for selected cameras, and stream for changing the license plate recognition settings** will appear instead of group boxes with FR settings' controls.

If the selected camera is used in some service but isn't allowed by the current FR license for this service, then **Selected camera for current service is not allowed by the license. Release FR service for this camera or for any other camera to keep a license for this one** comment will appear.

It is possible to switch the service name to **None** value for the selected camera but it’s not possible to switch service names for cameras with a **None** service name value when configured licenses number equals the total licenses number. In this case, the **Service name** field will be disabled for such cameras.

> “License (used / total)” field shows how many licenses are used by FR services and how many licenses are available. If license is unlimited “Unlimited” value is shown in this field.

Face detection settings

After the camera, its stream, and the FR detection service are selected, face detection settings can be adjusted. Face detection settings can be found in the **Detection Parameters** group box on the **FR settings** tab in the **Camera Settings** window.

Face detection settings are used for configuring the face recognition detector.

- **Region of interest** - define the area where the detections are made.
- **Max faces** – maximum number of faces to detect from the image. The value should be between 1 and 5.

- **Minimum confidence** – recognizer confidence level. If confidence for the detected face is below this threshold, then the face is ignored. Valid values are between 25% - 95%.
- **Minimum face height** – minimum face height in %. Valid values are from 5 to 50%%. Default value 10%.
- **Minimum face similarity** – If the similarity is greater than or equal to this value, then it is the same face. The value should be between 50% and 95%.
- **Same face event delay** – the number of seconds that should elapse before arising an event with the same face.
- **Device** – is used for inference. Available devices depend on the hardware of the actual service.
- **Thumbnail height** – the height of the thumbnail image in pixels. The value should be between 32 and 128 pixels.
- **Include thumbnail** – include detection source image thumbnail or not in returned data.
- **Include face images** – include face images or not in returned data.
- **Enable images HW decoding** – enable to decode input images with the most suitable computing platform (CUDA, DXVA or DirectX).

Save settings

Click the **OK** button with the green checkmark icon at the bottom of the **Camera Settings** window to save.

Click the **Cancel** button with the red cross icon to cancel saving FR settings and return to settings values loaded after opening the **System Manager** application.

When deleting stream settings for the selected camera and detection stream, the "None" value should be selected in the **Service name** Combobox for the selected camera and detection stream.

Influence on settings

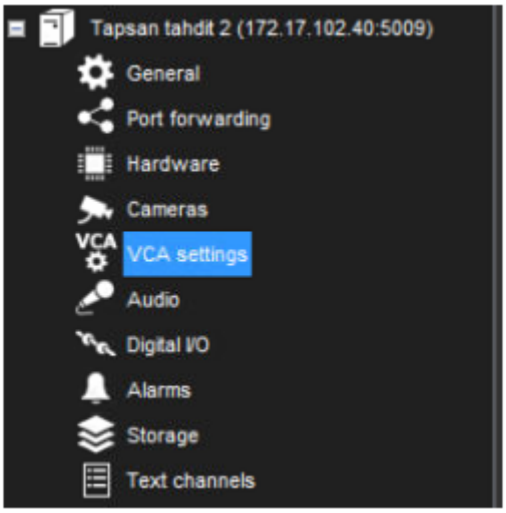
The following actions affect the service settings regardless of the actions on the **FR settings** tab:

1. *Deleting a recorder:* in case of deleting a recorder, all streams are deleted in the settings of all FR services that worked with the remote recorder and saving the FR settings.
2. *Deleting a camera:* in case of deleting a camera, the stream is deleted in the settings of all FR services that worked with this camera and saving FR settings. There is a rule - one camera with one stream can only be used by one FR service, but one FR service can work with multiple cameras.
3. *Changing the image size and compression type on the **Streams** subtab of the **General** tab:* in case of changing the resolution or compression type for the camera and stream, which are

present in the settings of any FR service, the FR service settings are changed, and saved when the **Camera Settings** window is closed.

4. *Changing the RTSP streaming settings in the* ***Streaming Settings*** *group of the* ***RTSP Server Streaming*** *tab:* in case of changing the "Password," "User Name", "RTSP Port", "Streaming Mode" (security type) for the selected camera and stream, which are present in the settings of any FR service, the FR service settings are changed and saved when the **Camera Settings** window is closed.
5. *Changing the image size in the* ***Device Settings*** *group of the* ***Video*** *tab in the* ***Hardware Settings*** *window:* in case of changing the resolution for the selected camera (here is possible to change the resolution for ***Recording*** stream only), which is present in the settings of any FR service, the FR service settings are changed and saved when the **Hardware Settings** window is closed.
6. *Changing the camera by clicking on the* ***Edit IP camera*** *button on the* ***Video*** *tab in the* ***Hardware Settings*** *window:* in case of changing the camera by clicking on the ***Edit IP camera*** *button* resolution and compression type for the new camera (for ***Recording*** stream only) will be rewritten in FR services settings, where camera ID is presented, the FR service settings are changed and saved when the **Hardware Settings** window is closed.

VCA settings



Check more details from Mirasys VCA Guide.

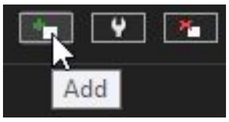
Audio .

Adding, Editing and Removing Audio Devices

The system supports three basic types of audio components: one-way analog and IP audio channels, two-way IP audio channels, and a single audio communication channel.

To configure audio devices:

1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Hardware** page from the menu.
3. Open the **Audio** tab.
4. Select the **Add**-option



5. Select the capture driver from the list.
6. Select one of these options:

- **Mono**. Select to use two mono channels.
- **Stereo**. Select to combine two mono channels into one stereo channel.
- Click **OK**.

Note: *IP camera-based IP audio input and output channels are added to the system primarily through the automated camera search tools.If an IP camera-based audio channel cannot be added through the camera search tools, or if the channel is added belatedly, follow the instructions above to add the audio channel.*

To edit an audio device:

- Open the **VMS Servers** tab.
- Select the correct server and open the **Hardware** page from the menu.
- Open the **Audio** tab.
- Select the audio channel.
- Click **Edit Audio Channel** in the lower right corner of the tab. The **Configure Audio** dialogue box is shown.

- Edit the information fields.
- Click **OK**.

To remove an audio device:

- Open the **VMS Servers** tab.
- Select the correct server and open the **Hardware** page from the menu.
- Open the **Audio** tab.
- Select the audio channel.
- Click **Remove Last Audio Channel from the List**in the lower right corner of the tab.**Note:** *You cannot remove an audio device from the middle of the list; only the most recently added audio device can be removed.*

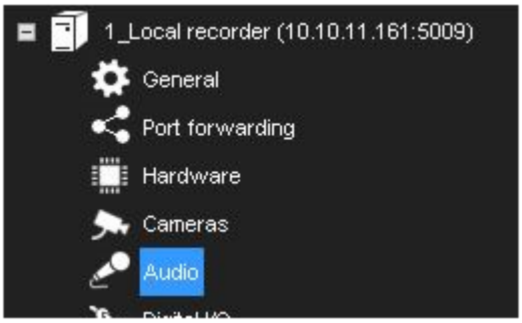
- The last audio device on the list is removed from the server.

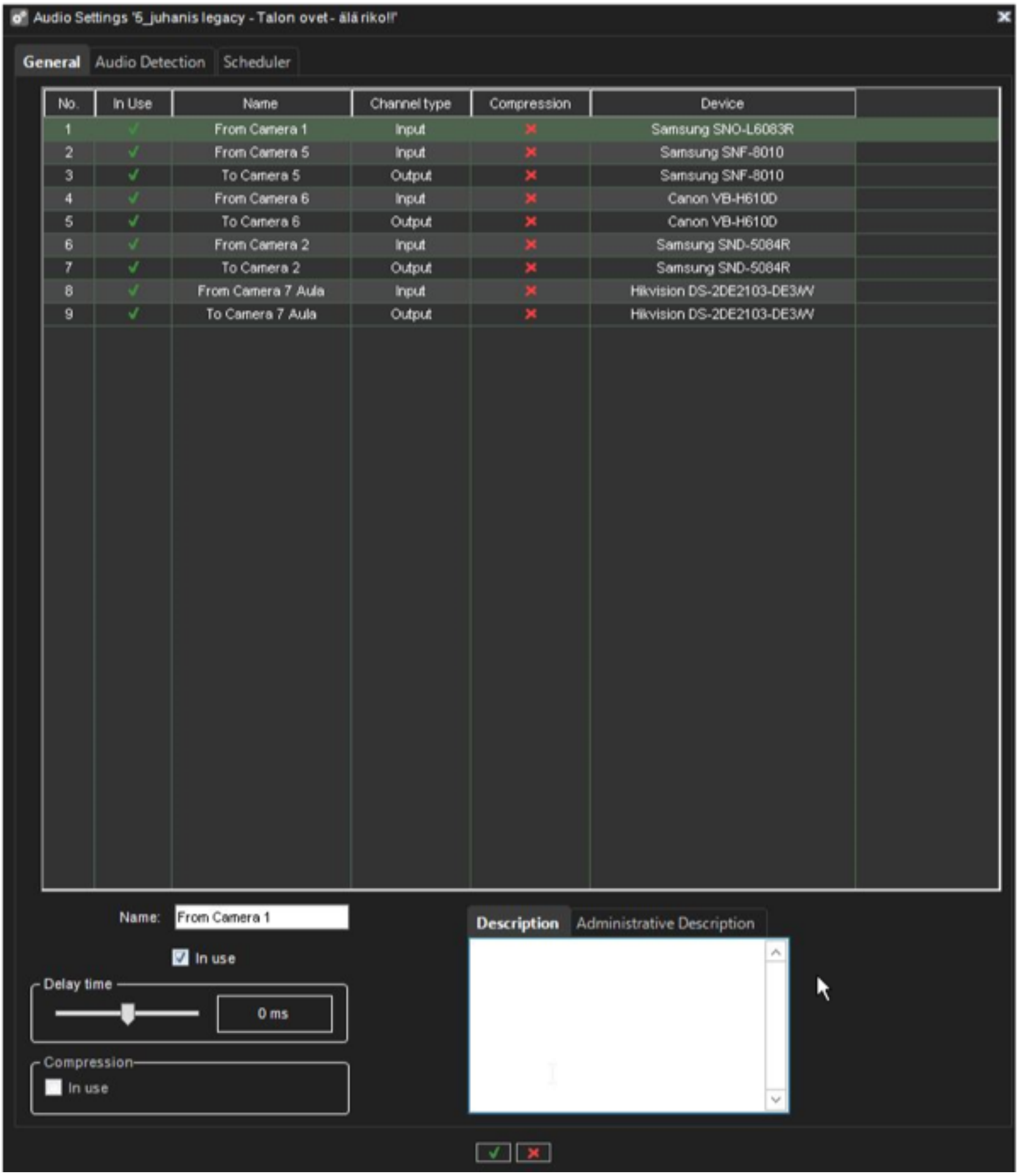
Audio Settings

The system supports three basic types of audio components:

- **One-way analogue and IP audio channels:** These include mainly camera-based and separate microphones.
- **Two-way IP audio channels:** Two-way IP audio channels require an IP camera with an audio input and output channel.
  a. Two-way IP audio channels are used for communication between the camera site and a Spotter client.
  b. Only one Spotter client can be used for communication at any time, but other clients in the system can listen to the channel and take over the communication if required.
  c. All communication that passes through a two-way IP audio channel is recorded in the system.
- **A single audio communication channel:** An older communication model. Each system contains one communication channel.
  - The drawback in using the audio communication channel is that the signal bypasses the server, meaning that the communication is not recorded in the system.

General Settings tab





Audio Settings '5_juhanis legacy - Talon ovet - älä rikol!'

No.	In Use	Name	Channel type	Compression	Device
1	✓	From Camera 1	Input	✗	Samsung SNO-L6083R
2	✓	From Camera 5	Input	✗	Samsung SNF-8010
3	✓	To Camera 5	Output	✗	Samsung SNF-8010
4	✓	From Camera 6	Input	✗	Canon VB-H610D
5	✓	To Camera 6	Output	✗	Canon VB-H610D
6	✓	From Camera 2	Input	✗	Samsung SND-5084R
7	✓	To Camera 2	Output	✗	Samsung SND-5084R
8	✓	From Camera 7 Aula	Input	✗	Hikvision DS-2DE2103-DE3/W
9	✓	To Camera 7 Aula	Output	✗	Hikvision DS-2DE2103-DE3/W

Name: From Camera 1

☑ In use

Delay time: 0 ms

Compression: □ In use

The **General** tab in the **Audio** page lists the basic settings of all audio channels:

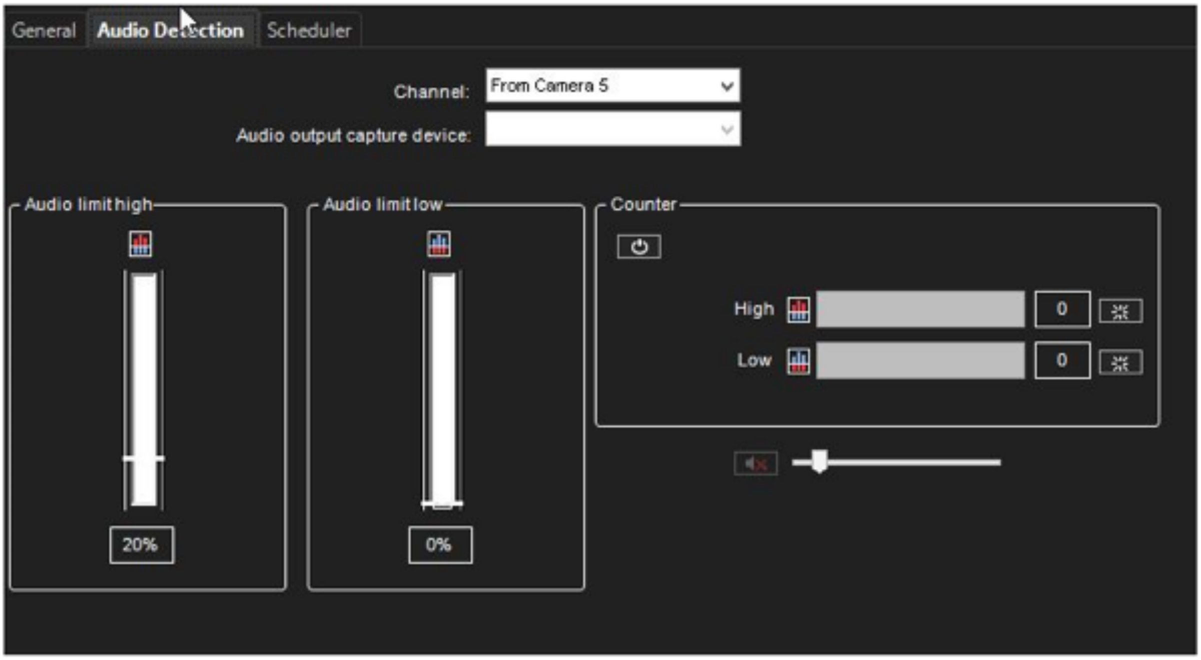
1. **No.** The number of the channel.

2. **In Use.** Shows if a channel is enabled or disabled.
3. **Name**. The name of the channel.
4. **Mono / Stereo**. Shows if a channel is a mono or stereo channel.
5. **Compression**. Shows if compression is on or off. A checkmark means that compression is used.
6. **Capture Driver**. Shows what capture driver is used. Select the driver in **Hardware Settings**.

To change general settings:

1. Select the channel from the list.
2. You can change these settings in the lower part of the window:
1. **Name**. The name of the channel.
2. **In use**. Select to enable the channel. Clear the check box to disable the channel.
3. **Delay time**. Sets the delay time in synchronizing the audio stream with other devices.
4. The delay time can be used to optimize the audio and video stream synchronization to, for example, enable better lip synchronization.
5. **Compression**. Select to use compression. Compressed audio files use less disk space, but the quality of the audio is a bit lower. Clear the check box to not use compression.
6. **Description**. Here you can type a description of the channel that will be shown to the users in the Spotter program.
7. **Administrative Description**. Here you can type a description of the channel that will be shown in the Spotter program to only system administrators.

Audio Detection



Channel: From Camera 5

Audio output capture device:

On the **Audio Detection** tab on the **Audio** page, set the high and low limits for audio detection.

The system records audio when the audio level exceeds the high limit.

In addition, you can set the system to give an alarm when the audio level exceeds the high limit or drops below the low limit.

To set the limits:

1. Select the audio channel from the list.
2. Click **Turn Audio Counter On/Off**.
   a. The system shows the audio level in the **Audio Limit High** and **Audio Limit Low** indicators, and the counters increment each time audio detection is activated.
   b. The top counter increments when the audio level exceeds the high limit. The lower counter increments when the audio level drops below the lower limit.
3. Set the high limit so that in usual conditions, the audio level stays below the limit.
   a. Audio detection is activated when the level exceeds the limit.
4. Set the low limit so that in usual conditions, the audio level stays above the limit.
   a. Audio detection is activated when the level drops below the limit.
5. To reset the counters, click the reset buttons.
6. Turn the counters off by clicking the **Turn Audio Counter On/Off** button.
7. To save the settings, click **OK**.

You can adjust the volume of audio and also mute the audio channel.

These settings are not saved; they only change how audio is played in the audio settings.

- **Mute**. Mutes the audio channel.
- **Adjust Volume**. Adjusts the audio volume.

Scheduler (Audio)

By default, audio is recorded when the detected level of audio exceeds the default detection limit (**Audio limit high**).

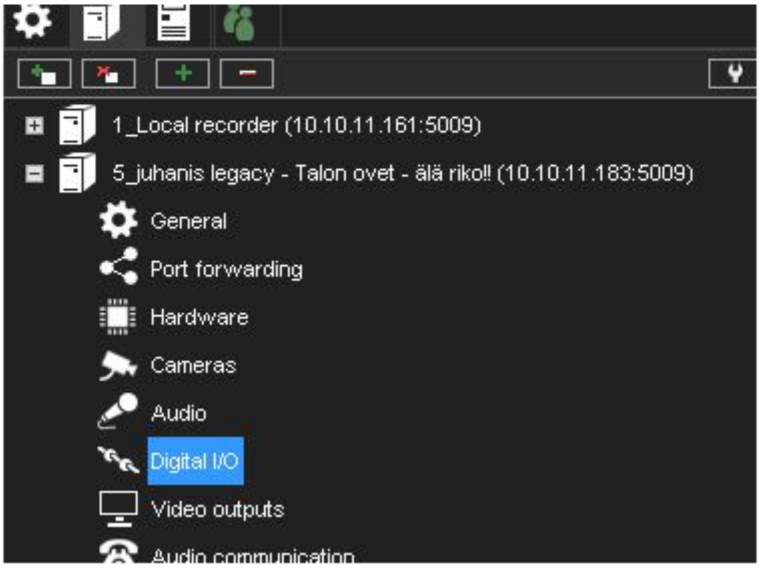
Similarly, to the video scheduler, it is possible to control the audio recording with the following options both for regular weeks and holidays.

1. **Off.** Audio is not recorded. However, possible alarms are recorded.
2. **Continuous.** All audio is recorded.
3. **Audio detection.** Audio is recorded when the measured level of audio exceeds the limit **Audio level is high.**

a. Set the limit on the Audio Settings

The functionality of this view is similar to the video scheduler.

Digital I/O


1_Local recorder (10.10.11.161:5009)

5_juhanis legacy - Talon ovet - älä riko!! (10.10.11.183:5009)

Digital I/O Settings

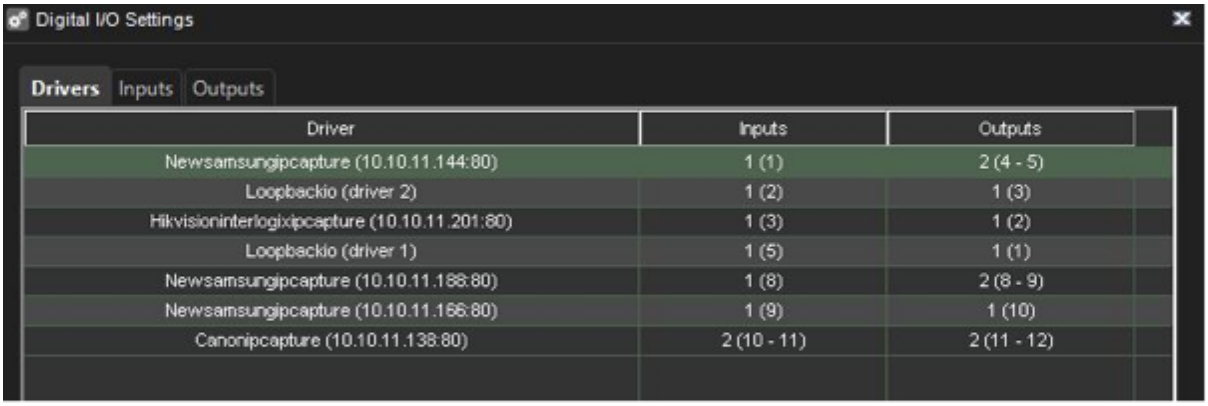
In **Digital I/O** settings, you can add digital input and output devices and configure the input and output settings.

These sections describe how to set up digital I/O devices.

Drivers

In addition to the default digital I/O drivers included in the system, new drivers can be added to the system by installing them as plugins.

Once an I/O device driver has been added to the system, the device can be configured and taken into use through the **Drivers** tab.

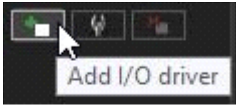


Digital I/O Settings

Driver	Inputs	Outputs
Newsamsungipcapture (10.10.11.144:80)	1 (1)	2 (4 - 5)
Loopbackio (driver 2)	1 (2)	1 (3)
Hikvisioninterlogixipcapture (10.10.11.201:80)	1 (3)	1 (2)
Loopbackio (driver 1)	1 (5)	1 (1)
Newsamsungipcapture (10.10.11.188:80)	1 (8)	2 (8 - 9)
Newsamsungipcapture (10.10.11.166:80)	1 (9)	1 (10)
Canonipcapture (10.10.11.138:80)	2 (10 - 11)	2 (11 - 12)

To take an I/O device driver into use:

1. If necessary, install the device driver package.
2. Open the **VMS Servers** tab.



1. Select the correct server and open the **Digital I/O** page from the menu.
2. Click **Add I/O driver** in the lower right corner of the screen.
3. Select the driver from the **Model** drop-down menu.
4. Configure the device settings in the **Properties** list.
5. To save the settings, click **OK**.

***Note:** After configuring a digital I/O device driver, you may need to configure the inputs and/or outputs.*

To edit I/O device driver settings:

1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Digital I/O** page from the menu.
3. Double click on the device driver you want to edit.
4. Edit the device settings in the **Properties** list.
5. To save the settings, click **OK**.

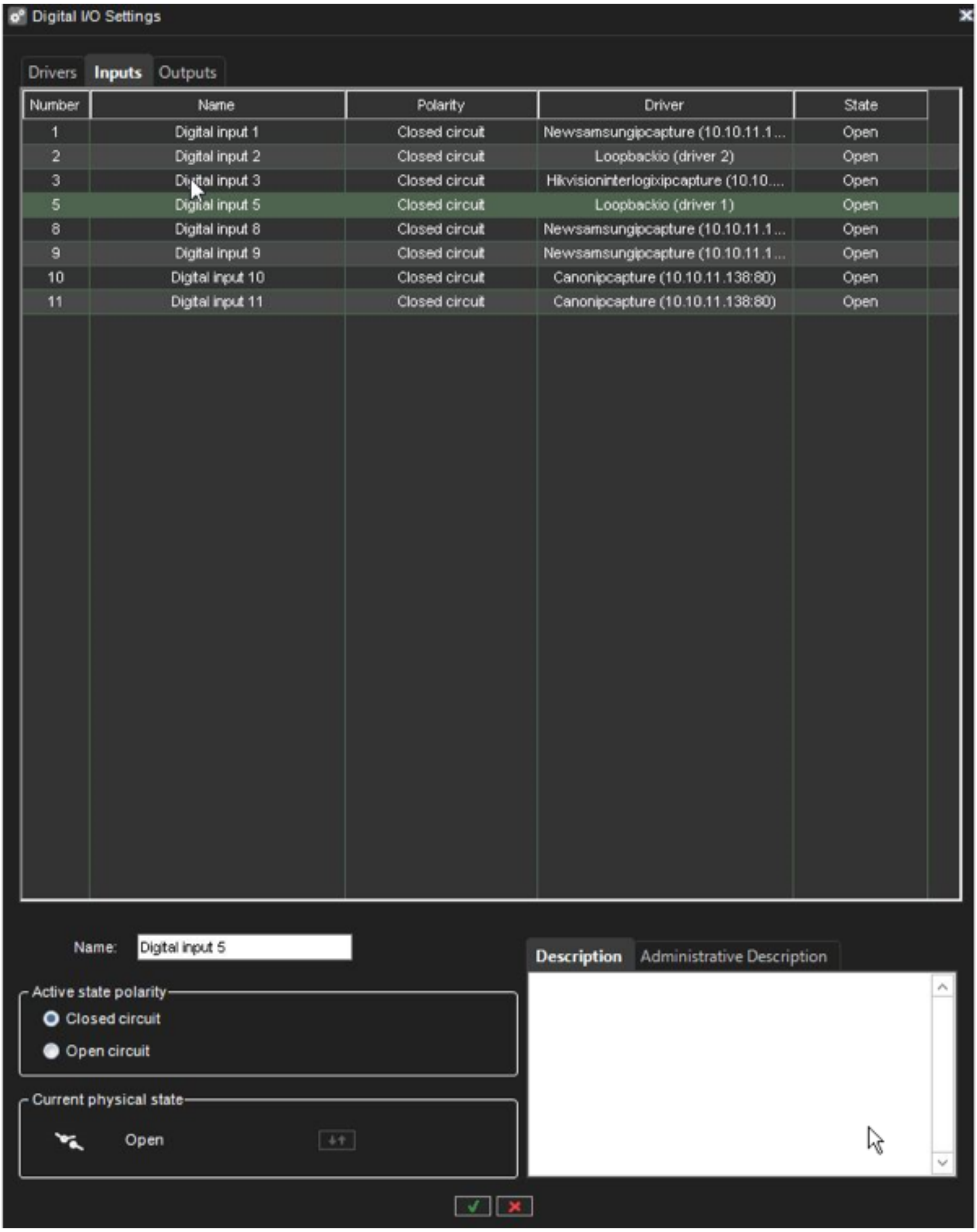
To delete an I/O device driver:

1. Open the **VMS Servers** tab.
2. Select the correct server and open the **Digital I/O** page from the menu.
3. Click on the I/O device driver you want to delete.
4. Click **Delete I/O driver** in the lower right corner of the screen.
5. Click **Ok** to confirm the deletion.

Digital Inputs

You can use digital inputs to activate alarms.

In digital input settings, set the polarity of the inputs. Set the alarm actions in alarm settings.



Digital I/O Settings

Number	Name	Polarity	Driver	State
1	Digital input 1	Closed circuit	Newsamsungipcapture (10.10.11.1...	Open
2	Digital input 2	Closed circuit	Loopbackio (driver 2)	Open
3	Digital input 3	Closed circuit	Hikvisioninterlogixipcapture (10.10....	Open
5	Digital input 5	Closed circuit	Loopbackio (driver 1)	Open
8	Digital input 8	Closed circuit	Newsamsungipcapture (10.10.11.1...	Open
9	Digital input 9	Closed circuit	Newsamsungipcapture (10.10.11.1...	Open
10	Digital input 10	Closed circuit	Canonipcapture (10.10.11.138:80)	Open
11	Digital input 11	Closed circuit	Canonipcapture (10.10.11.138:80)	Open

Name: Digital input 5

Active state polarity
- ● Closed circuit
- ○ Open circuit

Current physical state
Open

Name. To rename an input, select the input and then type a new name for the input in **Name.Active state polarity.** Select the input and then select if the input is activated when the circuit is opened or closed.

Current physical state. Shows the state of a relay in real-time (**Open** or **Closed**).

Description. Here you can type a description of the selected input shown to all users in the Spotter program.

Administrative Description. Here you can type a description of the selected input shown in the Spotter program to only system administrators.

Digital Outputs

In digital outputs, select if a relay is opened or closed (polarity) when the output is triggered.

Name. To rename an output, select the output and then type a new name for the output in **Name**.

Active state polarity. Select the output and then select if the output is closed or opened when it is activated.

Current physical state. Shows the state of a relay in real-time (**Open** or **Closed**).

Description. Here you can type a description of the selected output shown to all users in the Spotter program.

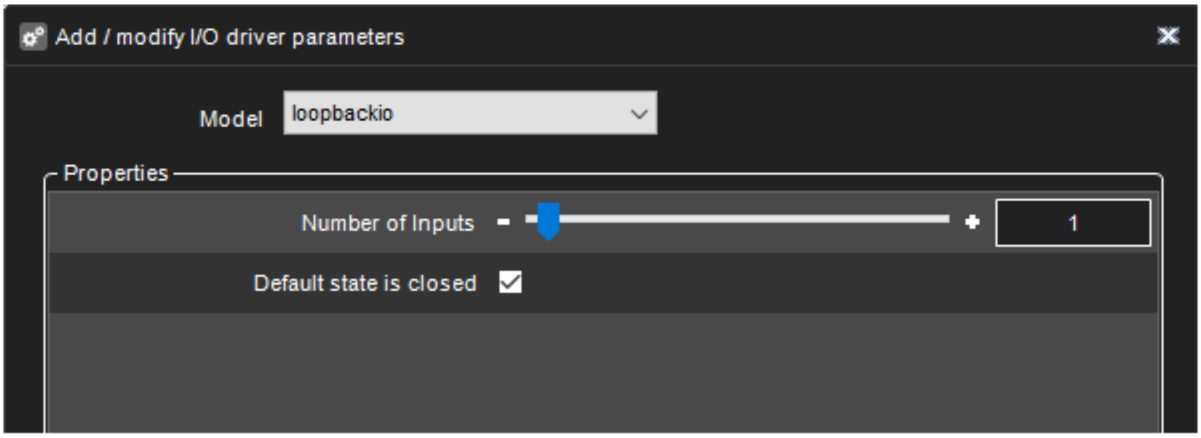
Administrative Description. Here you can type a description of the selected output shown in the Spotter program to only system administrators.

To test a digital output, click the **Change State (Toggle)** button.

LoopBack I/O

The LoopBack I/O allows you to create virtual I/O devices where the input is directly connected to the output.

This driver enables you to create buttons in the Spotter application to trigger alarms manually.



Add / modify I/O driver parameters

Model: loopbackio

Properties

Number of Inputs: 1

Default state is closed ☑

Logical I/O

With Logical I/O, it is possible to create actions based on the OR and AND operators.

The I/O driver emulates an external I/O that is connected to itself. Example:

For example, if the customer wants to confirm that an Automatic Number Plate Recognition (ANPR) event is triggered when a car is in front of the camera, the Logical I/O can be used to create a “rule” that results in action only when VCA detects a car, AND at the same time, there is an ANPR read event.

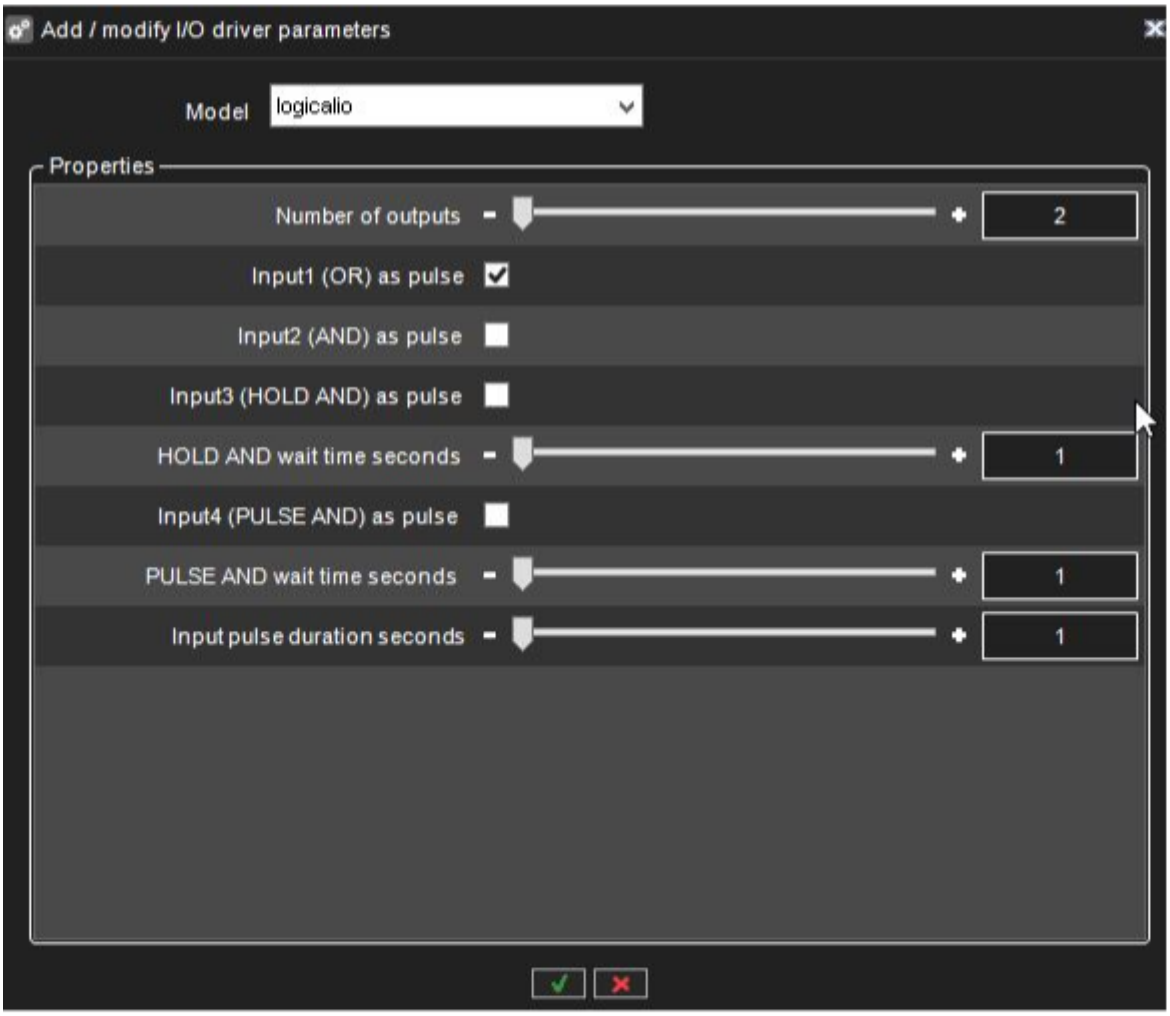
Another example could be that an entry “gate” with two doors only allows the second door to be opened when the first one is closed.

Logical I/O can be operated from the same interface as the rest of the Digital I/O in System Manager.

A license controls logical IO and countdown IO. If the license is not present, creating new IO will fail.

When a new Logical I/O is being added, the first option in the dialogue is how many output states are used as operands in the AND/OR decision making.

The minimum number is two, and the maximum is 32.



Model: logicalio

Number of outputs: 2

Input1 (OR) as pulse ☑

Input2 (AND) as pulse □

Input3 (HOLD AND) as pulse □

HOLD AND wait time seconds: 1

Input4 (PULSE AND) as pulse □

PULSE AND wait time seconds: 1

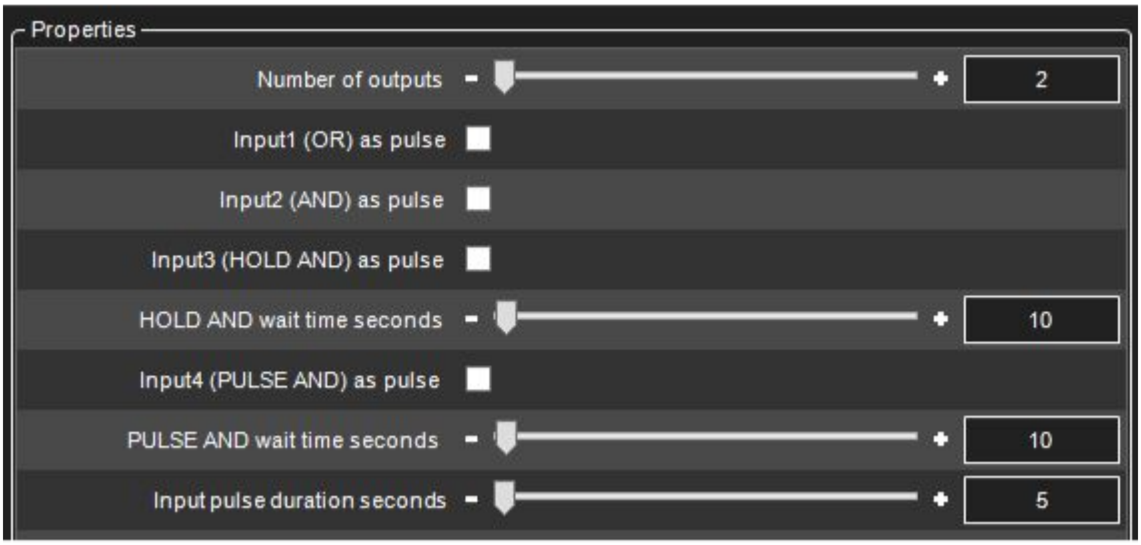
Input pulse duration seconds: 1

All Logical I/Os will automatically generate four inputs that can be used.

Input	Type
1	OR
2	AND

3	HOLD AND
4	PULSE AND

The following sections will describe the different inputs in more detail by using the below example:



Properties

Number of outputs: 2

Input1 (OR) as pulse ☐

Input2 (AND) as pulse ☐

Input3 (HOLD AND) as pulse ☐

HOLD AND wait time seconds: 10

Input4 (PULSE AND) as pulse ☐

PULSE AND wait time seconds: 10

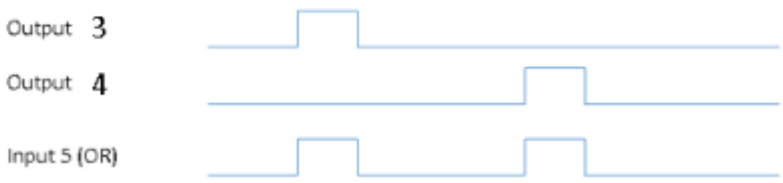
Input pulse duration seconds: 5

The example has 2 outputs that are the operands. These can be seen in the IO list as outputs 3 and 4.

The automatically created 4 inputs are seen in the list as inputs 5,6,7 and 8.

“OR” Input

The first input that the Logical I/O will generate is OR signal. If any of the outputs are on, the OR input will be turned on.

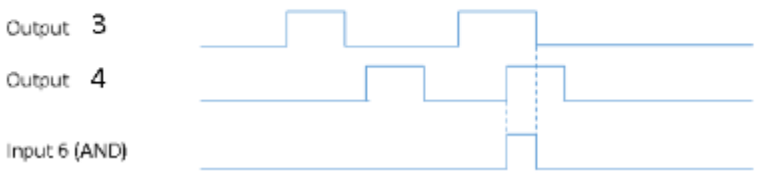


In our example, input 5 is the OR signal. If either output 3 OR output 4 are turned on, input 5 will be turned on as a result.

Input will remain on as long as any of the outputs remains on. (Unless pulse mode is selected, see below for details)

"AND" Input

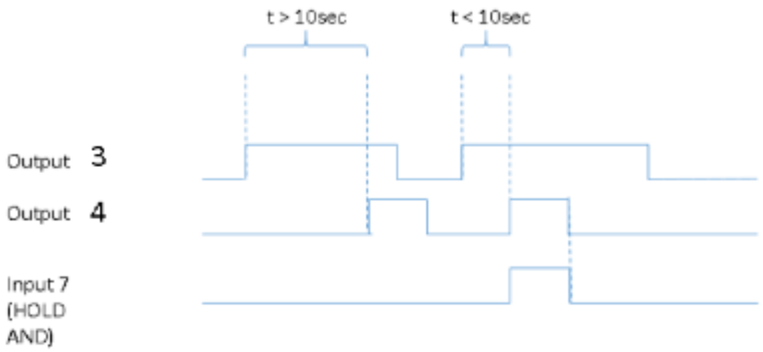
The second input is the AND signal. If all the outputs are on at the same time, the AND input will be turned on. In our example, if both outputs 3 and 4 are on simultaneously, input 6 will be turned on.



Input will remain on as long as all of the outputs remain on. (Unless pulse mode is selected, see below for details)

"HOLD AND" Input

HOLD AND input become active if all the outputs are active simultaneously, and the time from the first activation to the last activation is less than the time defined in the HOLD AND wait time slider.



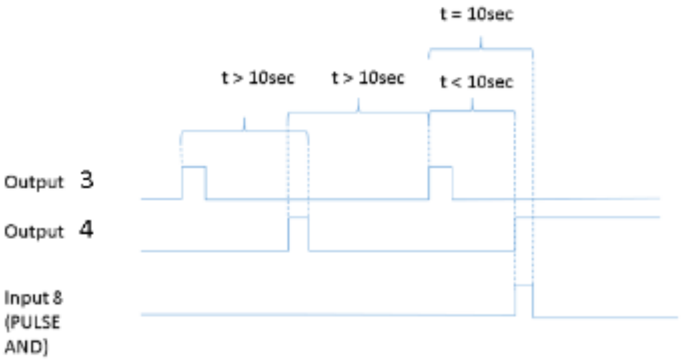
In our example, if output 3 is turned on, and then output 4 is turned on inside 10 seconds, input 7 will become active.

Input will remain on as long as all of the outputs remain on. (Unless pulse mode is selected, see below for details

"PULSE AND" Input

PULSE AND input will become active if all outputs *have been* active within a specified time.

In our example, if output 3 has been active inside 10 seconds, and output 4 becomes active, then input 8 will be turned on.

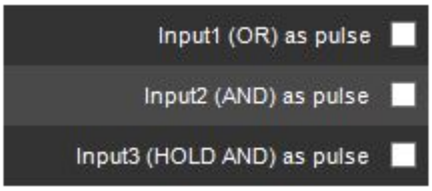


Input 8 remains until the specified time has elapsed from the oldest activating output (unless pulse mode is selected, see below for details).

In our example, when 10 seconds have elapsed from output 3 activation, input 8 will be turned off.

Pulse Mode For Inputs

For each of the four inputs, it is possible to define pulse mode to be in use.

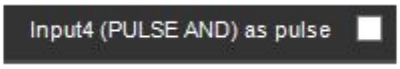


Input1 (OR) as pulse □

Input2 (AND) as pulse □

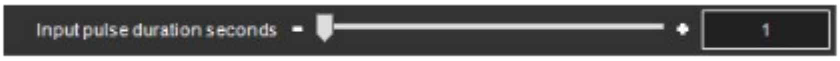
Input3 (HOLD AND) as pulse □

and



Input4 (PULSE AND) as pulse □

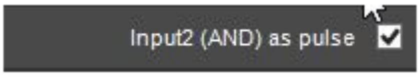
The pulse duration can also be adjusted.



Input pulse duration seconds 1

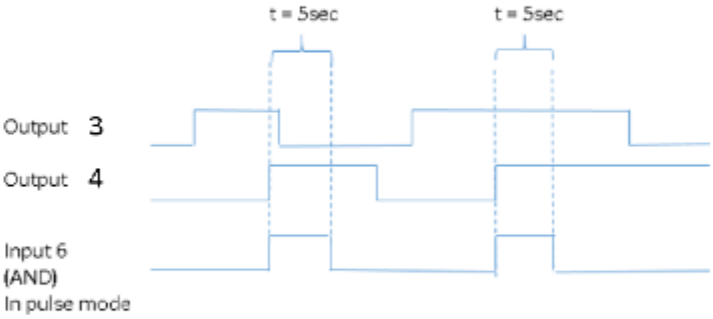
If the pulse mode is in use, the input will turn off after the set pulse duration.

If in our example, we would set the AND input to be in pulse mode like this:



Input2 (AND) as pulse ☑

It would mean behaviour like this:



Countdown I/O

With Countdown I/O, it is possible to create actions based on whether some events happen or do not happen at a defined period.

When a new Countdown I/O is created in System Manager, it automatically creates 4 inputs and 4 outputs.

Countdown I/O has two basic modes. The first two input/output pairs are of type 1, and the last two pairs are of type 2.

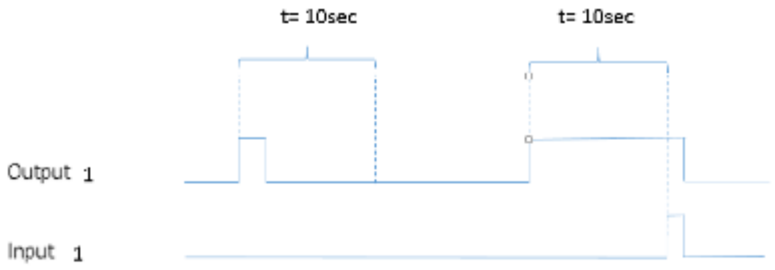
A license controls logical IO and countdown IO. If the license is not present, creating new IO will fail.

Event Duration Exceeded Mode (Type 1)

Firstly, it is possible to trigger an alarm if some event takes longer than the planned duration.

For example, let’s say the time is 10 seconds. If output one is triggered and stays active for less than the defined duration, there is no alarm.

If the output is triggered and stays active for longer than the defined duration, there is an alarm.



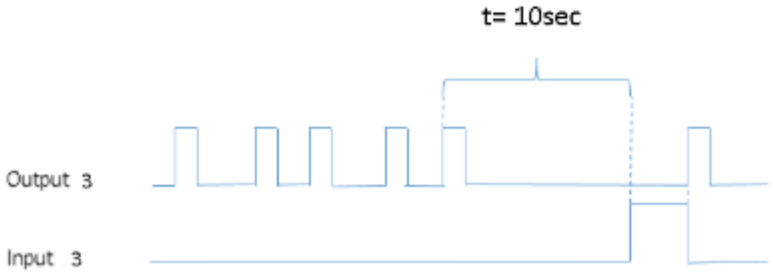
When creating a new Countdown I/O, the first two input-output pair is of this type.

Expected Trigger Mode (Type 2)

Secondly, it is possible to trigger an alarm if an expected pulse is not received inside the defined time.

For example, the time is 10 seconds, and we expect the regular operation to get pulses from output 3 every 2-3 seconds.

When the pulse is missing for longer than 10 seconds, the input state is changed to active. It stays active until the next output trigger is received.



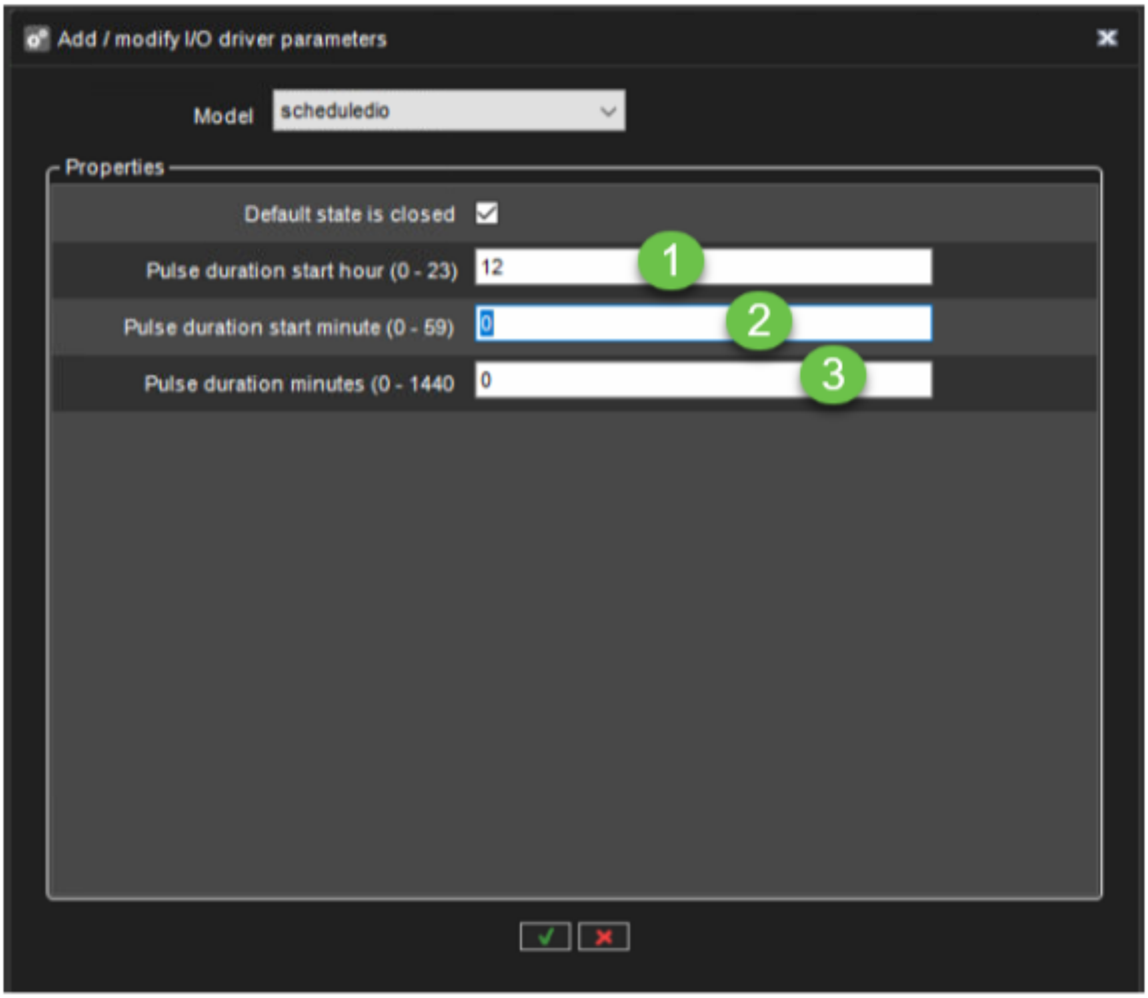
When creating a new Countdown I/O, the last input-output pair is of this type.

Scheduled IO

With the Scheduled IO is possible to create a schedule for any digital output, which are connected to the VMS server.

Only the same VMS server digital outputs can be scheduled.

1. Set Pulse duration start an hour
2. Set Pulse duration start minute
3. Set Pulse duration minutes



Add / modify I/O driver parameters

Model: scheduledio

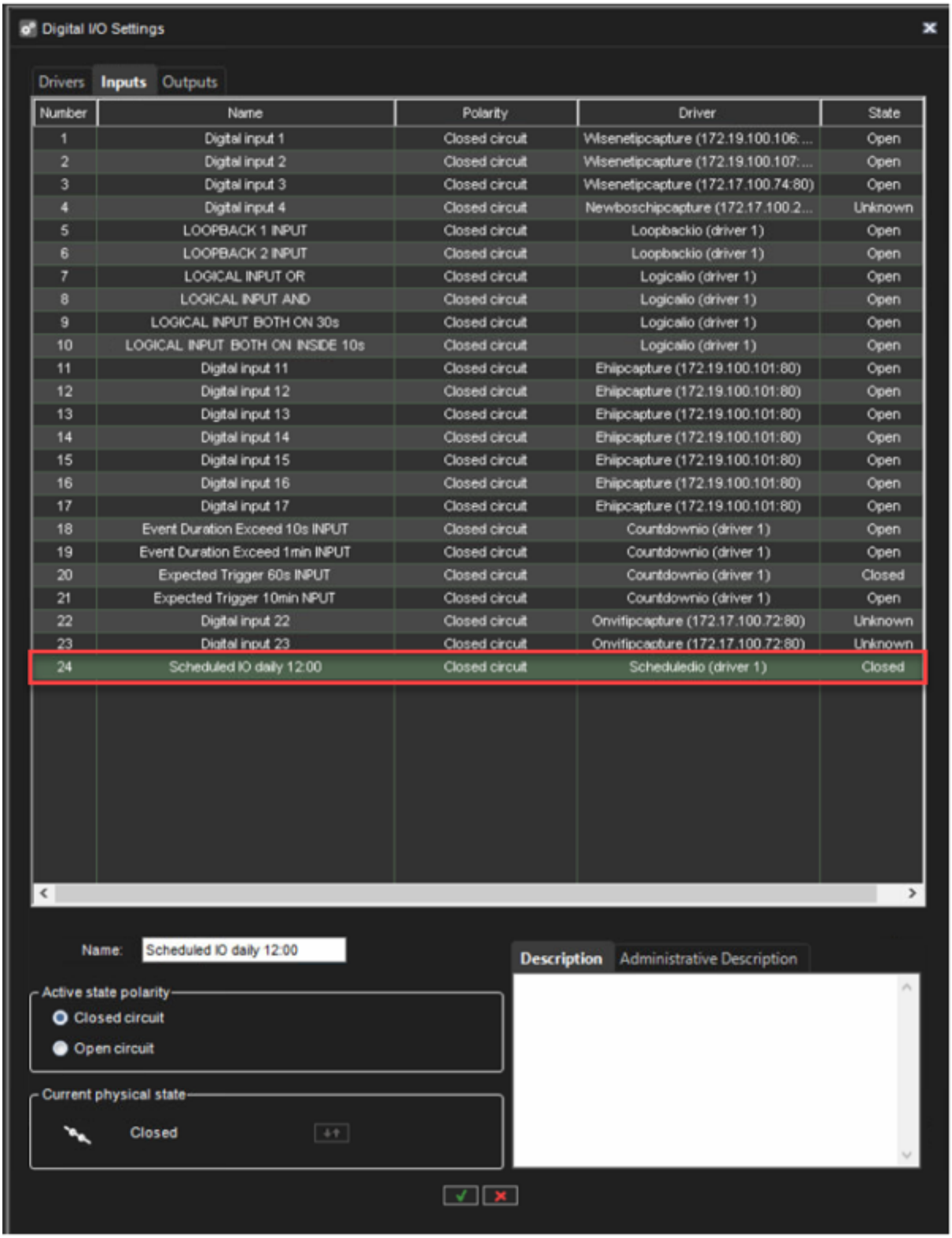
Properties

Default state is closed ☑

Pulse duration start hour (0 - 23): 12

Pulse duration start minute (0 - 59): 0

Pulse duration minutes (0 - 1440: 0



Number	Name	Polarity	Driver	State
1	Digital input 1	Closed circuit	Wisenetipcapture (172.19.100.106:...	Open
2	Digital input 2	Closed circuit	Wisenetipcapture (172.19.100.107:...	Open
3	Digital input 3	Closed circuit	Wisenetipcapture (172.17.100.74:80)	Open
4	Digital input 4	Closed circuit	Newboschipcapture (172.17.100.2...	Unknown
5	LOOPBACK 1 INPUT	Closed circuit	Loopbackio (driver 1)	Open
6	LOOPBACK 2 INPUT	Closed circuit	Loopbackio (driver 1)	Open
7	LOGICAL INPUT OR	Closed circuit	Logicalio (driver 1)	Open
8	LOGICAL INPUT AND	Closed circuit	Logicalio (driver 1)	Open
9	LOGICAL INPUT BOTH ON 30s	Closed circuit	Logicalio (driver 1)	Open
10	LOGICAL INPUT BOTH ON INSIDE 10s	Closed circuit	Logicalio (driver 1)	Open
11	Digital input 11	Closed circuit	Ehiipcapture (172.19.100.101:80)	Open
12	Digital input 12	Closed circuit	Ehiipcapture (172.19.100.101:80)	Open
13	Digital input 13	Closed circuit	Ehiipcapture (172.19.100.101:80)	Open
14	Digital input 14	Closed circuit	Ehiipcapture (172.19.100.101:80)	Open
15	Digital input 15	Closed circuit	Ehiipcapture (172.19.100.101:80)	Open
16	Digital input 16	Closed circuit	Ehiipcapture (172.19.100.101:80)	Open
17	Digital input 17	Closed circuit	Ehiipcapture (172.19.100.101:80)	Open
18	Event Duration Exceed 10s INPUT	Closed circuit	Countdownio (driver 1)	Open
19	Event Duration Exceed 1min INPUT	Closed circuit	Countdownio (driver 1)	Open
20	Expected Trigger 60s INPUT	Closed circuit	Countdownio (driver 1)	Closed
21	Expected Trigger 10min NPUT	Closed circuit	Countdownio (driver 1)	Open
22	Digital input 22	Closed circuit	Onvifipcapture (172.17.100.72:80)	Unknown
23	Digital input 23	Closed circuit	Onvifipcapture (172.17.100.72:80)	Unknown
24	Scheduled IO daily 12:00	Closed circuit	Scheduledio (driver 1)	Closed

Name: Scheduled IO daily 12:00

Active state polarity
- ● Closed circuit
- ○ Open circuit

Current physical state: Closed

Properties

HTTP Method(Opened)

- GET
- PUT
- POST
- DELETE

URL(Opened)

Content(Opened)

User(Opened)

Password(Opened)

HTTP Method(Closed)

- GET
- PUT
- POST
- DELETE

URL(Closed)

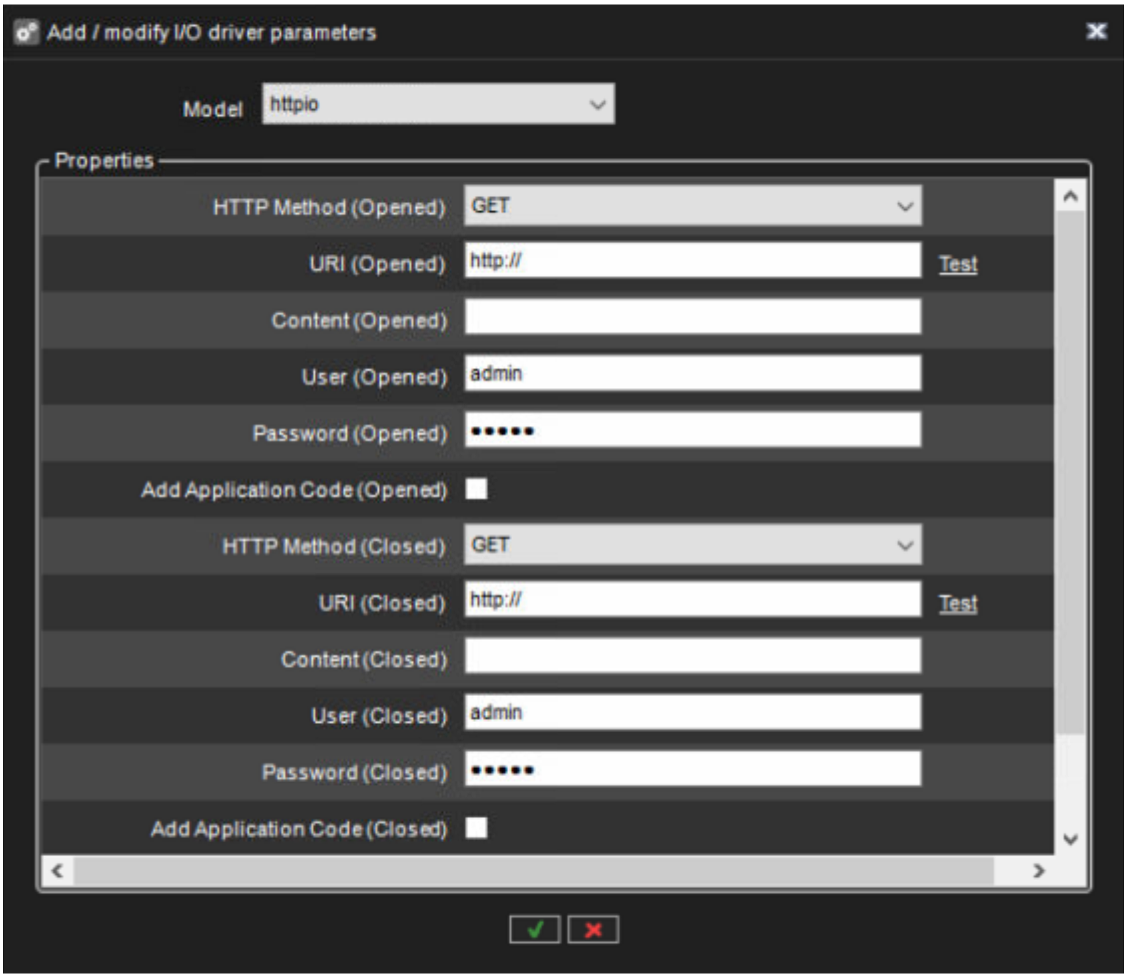
Content(Closed)

User(Closed)

Password(Closed)

Authentication

- BASIC
- DIGEST



Add / modify I/O driver parameters

Model: httpio

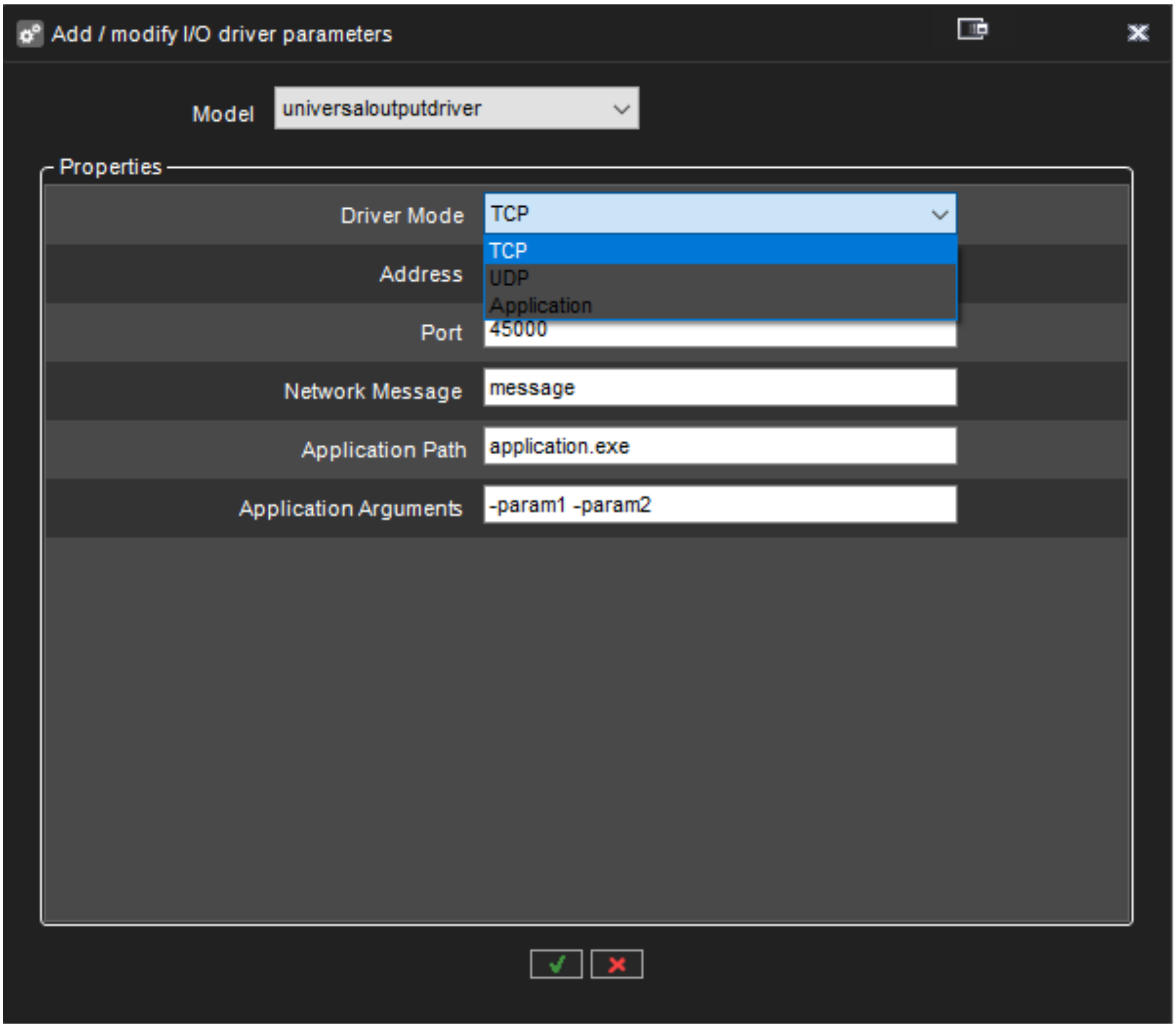
Properties

HTTP Method (Opened)	GET
URI (Opened)	http://
Content (Opened)	
User (Opened)	admin
Password (Opened)	•••••
Add Application Code (Opened)	□
HTTP Method (Closed)	GET
URI (Closed)	http://
Content (Closed)	
User (Closed)	admin
Password (Closed)	•••••
Add Application Code (Closed)	□

UniversalOutputDriver

This driver enables you to send data to 3rd party systems or start applications on the server or remote systems.

Please see additional documentation for this driver from our extranet or contact support.



Add / modify I/O driver parameters

Model: universaloutputdriver

Properties

Driver Mode: TCP

Address

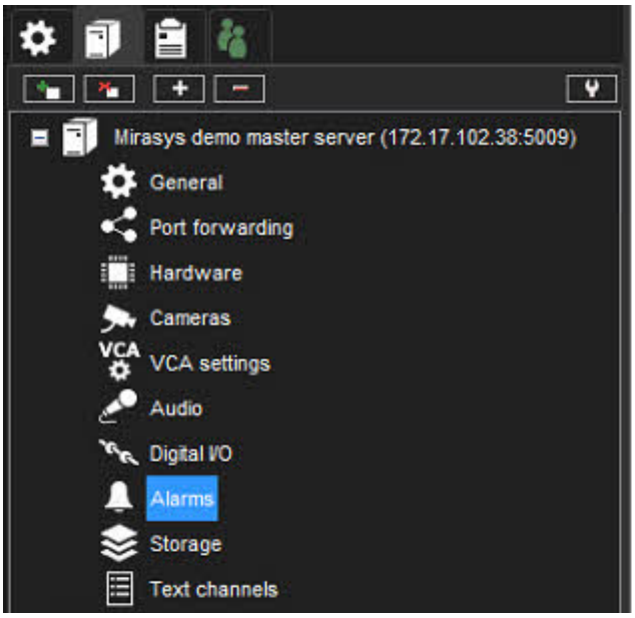
Port: 45000

Network Message: message

Application Path: application.exe

Application Arguments: -param1 -param2

Alarms



Alarm Settings

The alarm management tools enable the creation of server-specific alarms based on various triggers based on motion, sound level or specific text data triggers.

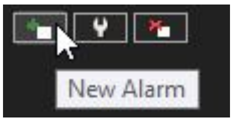
In addition, the triggers can include custom-made third-party triggers.

Alarms can be created, edited and deleted through the **Alarms** screen in the **VMS Servers** tab.

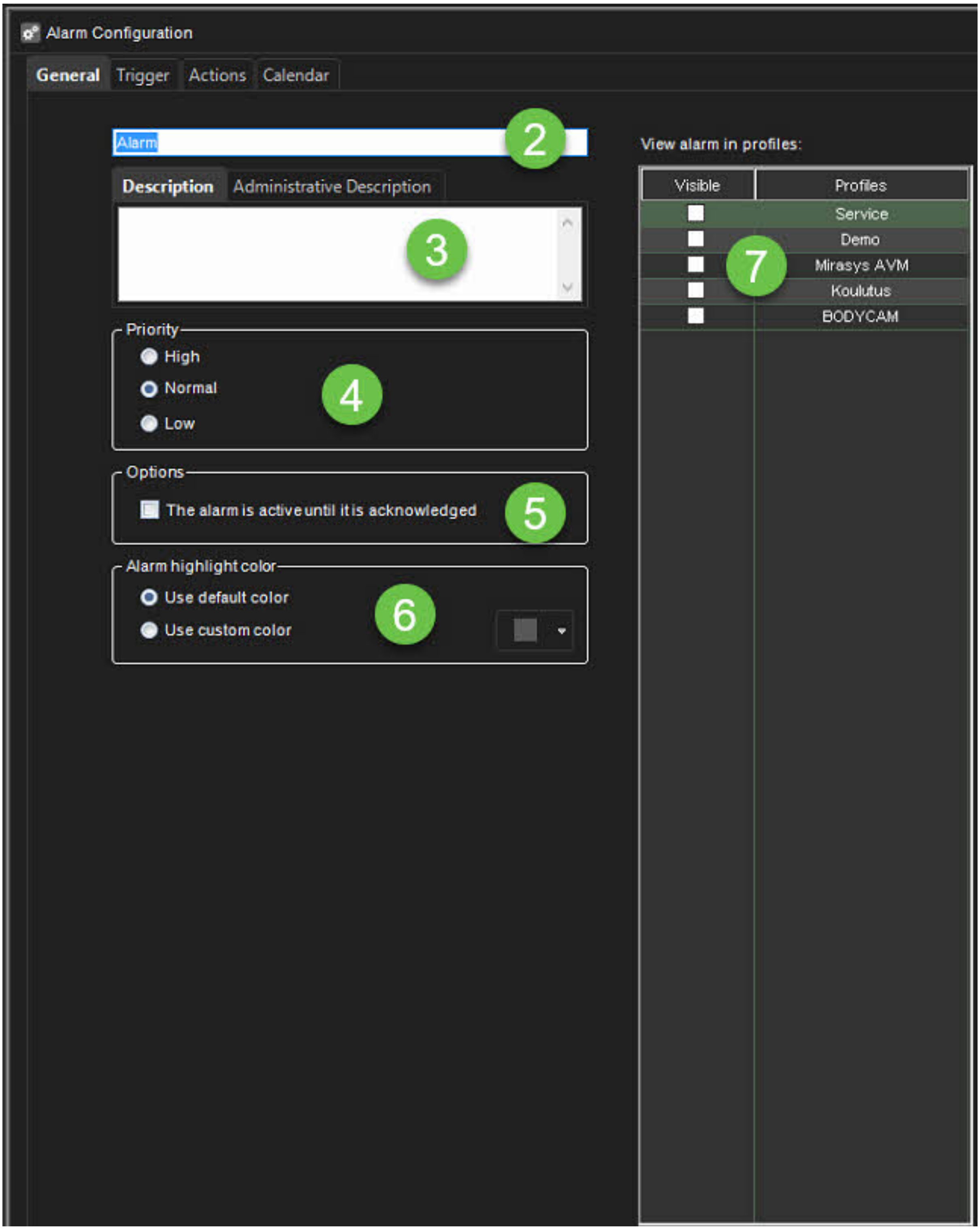
Adding a New Alarm

General

- Click New Alarm at the lower-left corner of the Alarms screen.



- Type the name of the new alarm in the **Name** field.
- Type the **description** and **administrative description** of the new alarm to the respective fields below the **Name** field.
- Select whether the alarm is of **high**, **average** or **low priority**. The priority is used to define the order in which alarms are executed in case of multiple simultaneous alarms.
- Select **The Alarm is active until it is acknowledged** to create the alarm as continuous; if the option is selected, the alarm will continue until a user acknowledges it through the **Spotter** application.
- **Alarm highlight colour** allows administrators to define a custom colour for each alarm separately.
- In the **View Alarms in Profiles** menu, select the profiles in which the alarm will be used. *Note: Alarms can also be added to profiles through the **Profiles** tab.*



Alarm Configuration

General | Trigger | Actions | Calendar

Alarm

Description | Administrative Description

Priority

○ High

● Normal

○ Low

Options

☐ The alarm is active until it is acknowledged

Alarm highlight color

● Use default color

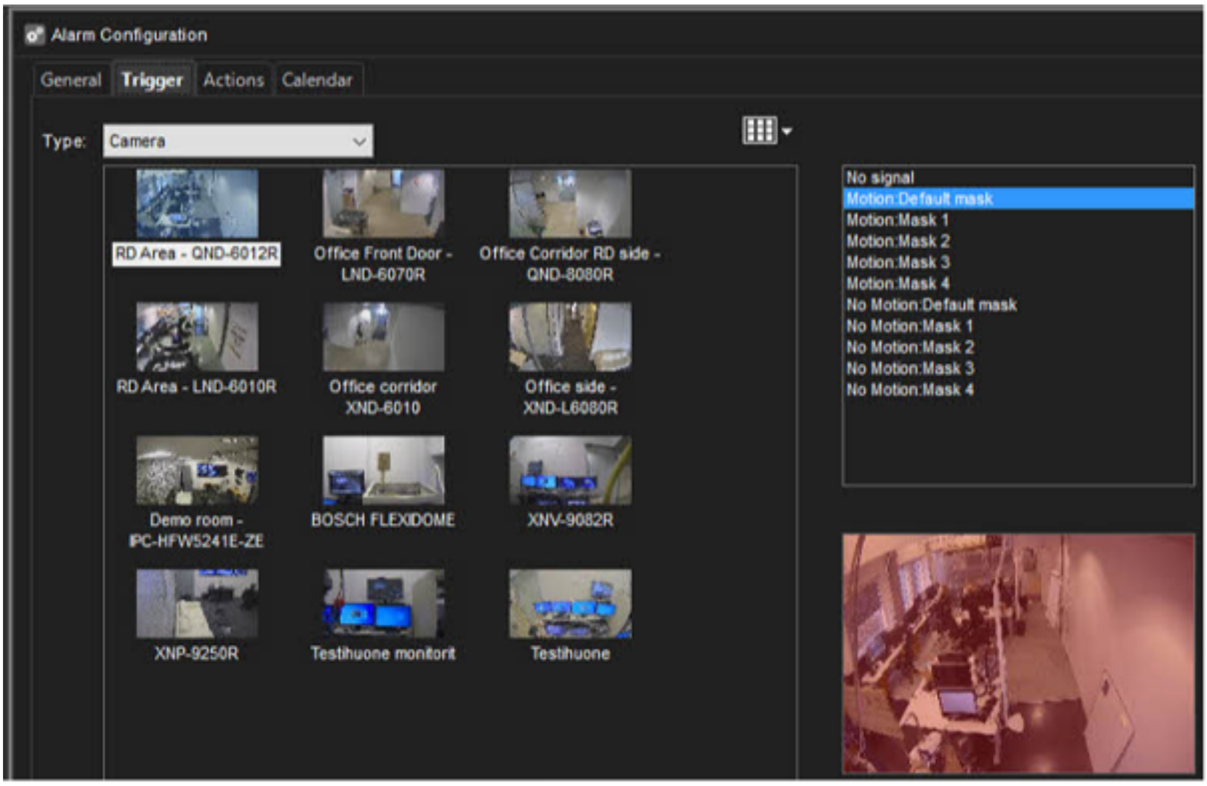
○ Use custom color

View alarm in profiles:

Visible	Profiles
☐	Service
☐	Demo
☐	Mirasys AVM
☐	Koulutus
☐	BODYCAM

Trigger

8. Open the **Trigger** tab. The **Trigger** tab is used to define the triggers that start the alarm event.



Type: Camera

9. Select the trigger type from the **Type** drop-down menu.

1. Camera
2. Audio
3. Metadata
4. Text data
5. Digital input

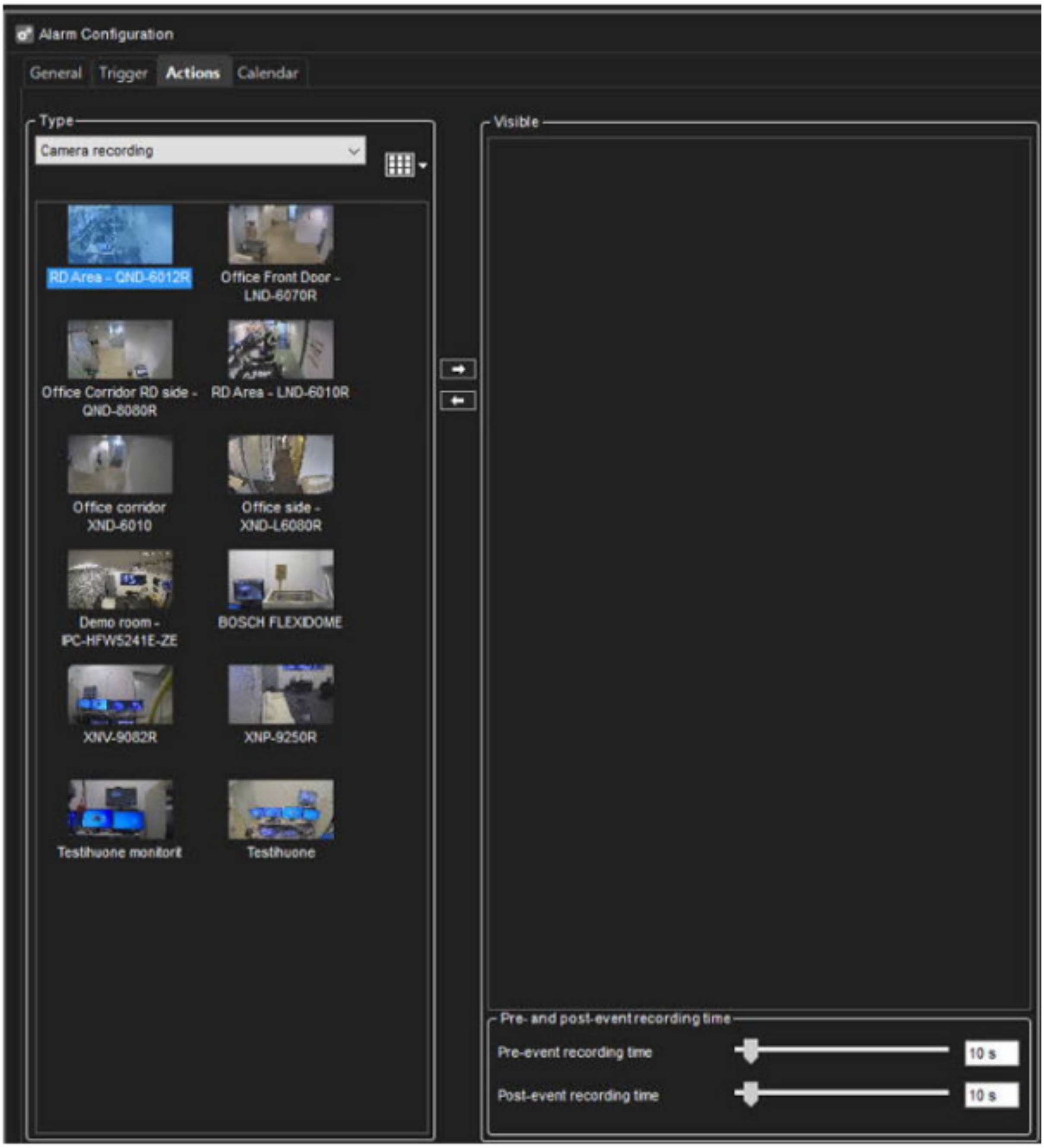
10. Select the device that will trigger the alarm from the device list below the **Type** drop-down menu.

11. Select the triggering condition from the condition list on the right side of the screen.

- For camera-based triggers, you can select the mask used in motion detection to trigger the alarm.
- For audio-based triggers, you can set the alarm to trigger based on a high or low audio level.
- For text data based (e.g., VCA, metadata, etc.) triggers, you can set the alarm to trigger based on a text data string.
  In addition, you can set an optional alarm ending trigger by marking **Define ending input** and selecting a string for ending the alarm.
- For digital input-based triggers, the alarm is triggered based on the change of the input's polarity.

Actions

12. Open the **Actions** tab. The **Actions** tab is used to define the actions performed by the alarm when it is triggered.



13. Select the action type from the **Type** drop-down menu. The action type defines the basic functionality of the alarm.

Action Types and Settings

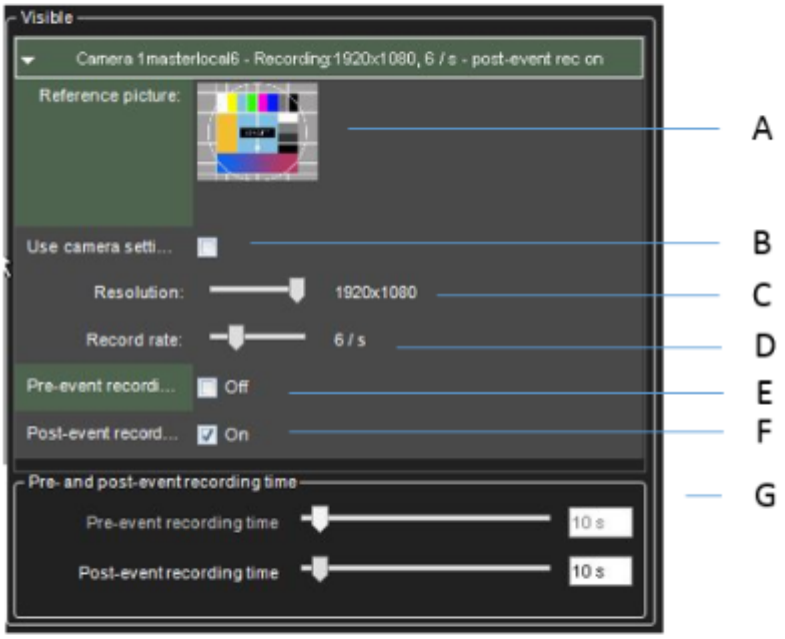
The list below contains the default action types and their parameters. Some of the action types listed above may not be available on all systems.

Note: *In addition to the default actions, the system may include alarm actions installed through third-party modules.*

Camera Recording

Camera recording is the default action for cameras. When an alarm that contains this action type is triggered, the recording settings defined by the alarm type will be used instead of the camera's default settings.

In **Spotter**, if alarm pop-up windows are enabled for the user profile, devices used with the **Camera recording** action are displayed in the alarm pop-up view when the alarm is triggered.



Visible

Camera 1masterlocal6 - Recording 1920x1080, 6 / s - post-event rec on

Reference picture:

Use camera setti... □

Resolution: 1920x1080

Record rate: 6 / s

Pre-event recordi... □ Off

Post-event record... ☑ On

Pre- and post-event recording time

Pre-event recording time 10 s

Post-event recording time 10 s

The action includes the following fields and parameters:

A) Reference picture. This static field contains the reference picture (image) of the camera.

B) Use camera settings. The alarm recording will be performed using the camera-specific resolution and record rate setting by marking this checkbox.

C) Resolution. Use the slider to change an IP camera's resolution during alarm recording. The slider is active only for IP cameras.

D) Record rate. Use the slider to change the camera's IPS rate during alarm recording. The slider is inactive if the **Use camera settings** checkbox is marked.

E) Pre-event recording. Mark this checkbox to set the pre-event recording on. The duration of the pre-event recording can be set through the **Pre-event recording time** slider.

F) Post-event recording. Mark this checkbox to set post-event recording on. The duration of the pre-event recording can be set through the **Post-event recording time** slider.

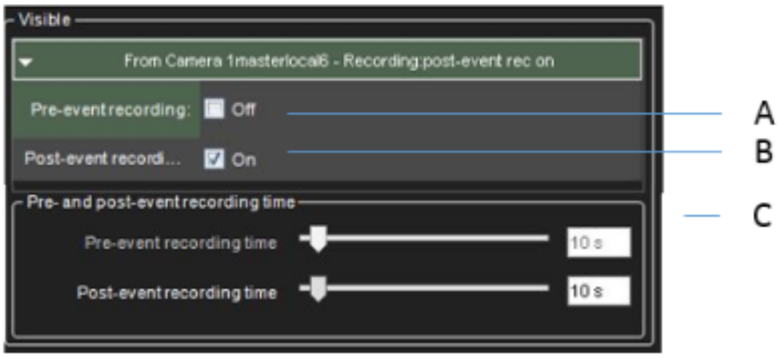
G) Pre- & post-event recording duration. These sliders can be used to set the pre-and post-event recording durations for the action. The sliders are active only if pre-event and/or post-event recording has been activated.

Note *All devices (cameras and microphones) are connected to the alarm and have their pre-and post-event recording activated to share the same pre-and post-event recording durations.*

Audio Recording

Audio recording is the default action for microphones. When an alarm that contains this action type is triggered, the recording settings defined by the alarm type will be used instead of the microphone's default settings.

In **Spotter**, if alarm pop-up windows are enabled for the user profile, devices used with the **Audio recording** action are displayed in the alarm pop-up view when the alarm is triggered.



Visible

From Camera 1masterlocal6 - Recording:post-event rec on

Pre-event recording: ☐ Off

Post-event recordi... ☑ On

Pre- and post-event recording time

Pre-event recording time 10 s

Post-event recording time 10 s

The action includes the following fields and parameters:

A) Pre-event recording. Mark this checkbox to set the pre-event recording on. The duration of the pre-event recording can be set through the **Pre-event recording time** slider.

B) Post-event recording. Mark this checkbox to set post-event recording on. The duration of the pre-event recording can be set through the **Post-event recording time** slider.

C) Pre- & Post Recording duration. These sliders can be used to set the pre-and post-event recording durations for the action. The sliders are active only if pre-event and/or post-event recording has been activated.

Note: *All devices (cameras and microphones) connected to the alarm and have their pre-and post-event recording activated to share the same pre-and post-event recording durations.*

Digital output

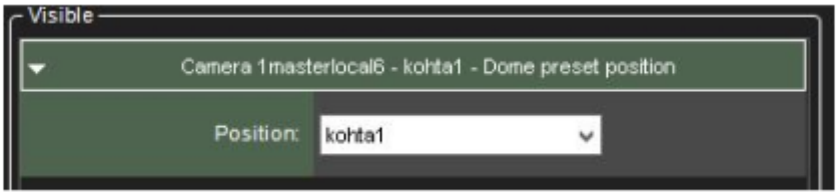
The **digital output** is the default action for digital I/O devices. When an alarm that contains this action type is triggered, the I/O device is activated.

Note: *Even though the* ***Pre- & Post Recording duration*** *sliders are displayed for the action type, they do not affect the functionality of the action.*

PTZ (Dome) Preset Position

*The **PTZ preset position** action can be used to set a PTZ camera to a specified preset position. When an alarm that contains this action type is triggered, the PTZ camera will automatically move to the selected preset position. Please see Mirasys VMS Spotter User's Guide for information on setting PTZ camera preset positions.*

It should be noted that this action moves the PTZ camera to a preset position but does not result in the video feed from the PTZ camera being displayed in the alarm view in the client application unless other alarm actions, such as **Camera recording,** has been selected for the PTZ camera.



Visible

Camera 1masterlocal6 - kohta1 - Dome preset position

Position: kohta1

The action includes the following fields and parameters:

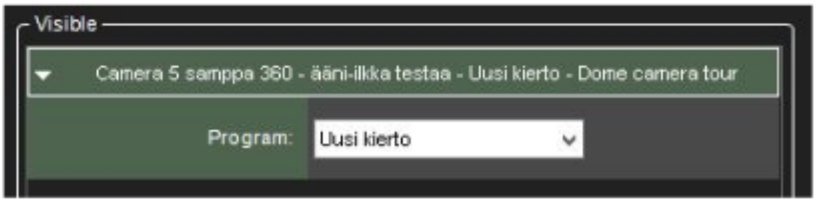
- **Position**. Use the drop-down menu to select the preset position to which the PTZ camera will move during the alarm.

Note: *Even though the **Pre- & Post Recording duration** sliders are displayed for the action type, they do not affect the functionality of the action.*

PTZ (Dome) Camera Tour

The **PTZ camera tour** action can be used to set a PTZ camera to start a pre-programmed PTZ camera tour. When an alarm that contains this action type is triggered, the selected PTZ camera tour is started. Please see *Mirasys VMS Spotter User's Guide* for information on setting PTZ camera tours.

It should be noted that this action starts the PTZ camera tour but does not result in the video feed from the PTZ camera being displayed in the alarm view in the client application unless other alarm actions, such as **Camera recording,** has been selected for the PTZ camera.



Visible

Camera 5 samppa 360 - ääni-ilkka testaa - Uusi kierto - Dome camera tour

Program: Uusi kierto

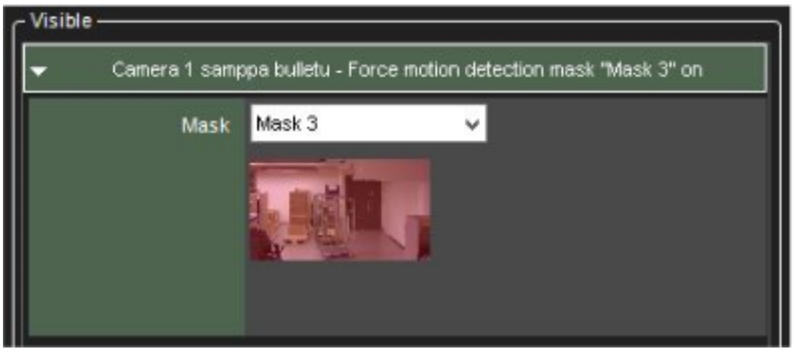
The action includes the following fields and parameters:

- **Program**. Use the drop-down menu to select the PTZ camera tour, starting when the alarm is triggered.

Note: *Even though the* ***Pre- & Post Recording duration*** *sliders are displayed for the action type, they do not affect the functionality of the action.*

Set Motion Detection Mask

The **Set motion detection mask** action can change the motion detection mask used by a specific camera during the alarm. When the alarm occurs, the motion detection mask used for the designated camera is changed to the alarm specific mask. After the alarm ends, the system restores the default mask.



Visible

Camera 1 samppa bulletu - Force motion detection mask "Mask 3" on

Mask: Mask 3

The action includes the following fields and parameters:

- **Mask**. Use the drop-down menu to select the motion detection mask that will be used during the alarm.

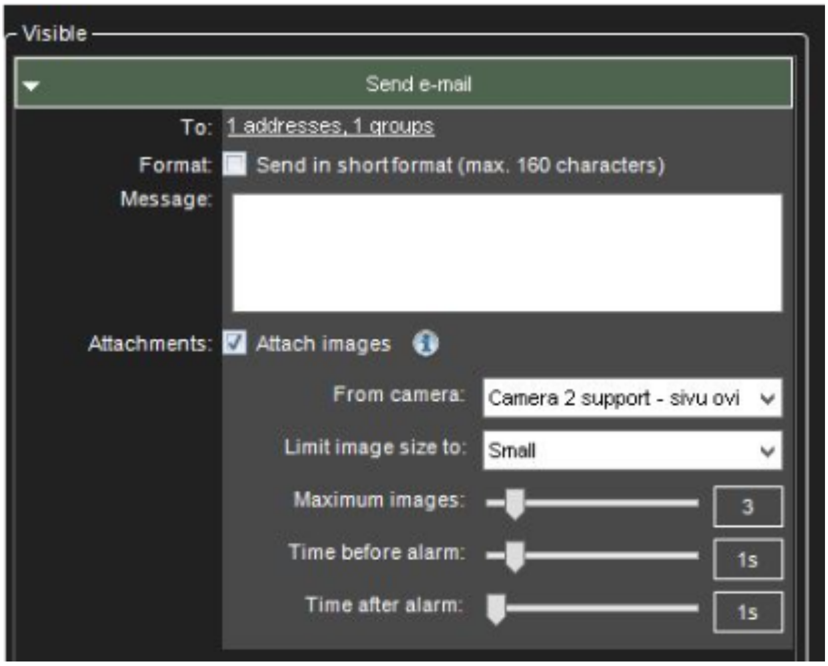
Note: *Even though the* ***Pre- & Post Recording duration*** *sliders are displayed for the action type, they do not affect the functionality of the action.*

Send E-Mail

The **Send e-mail** action can be used to send e-mail to any email address or group configured in the **E-mail settings** in the **System** tab.

You can choose which recipient or group should receive the alarm.

You can also include one or more unscaled or scaled-down images in the alarm email. To do this, uncheck the **Send in a short format** -option and check the **Attach images** –option



Visible

Send e-mail

To: 1 addresses, 1 groups

Format: □ Send in short format (max. 160 characters)

Message:

Attachments: ☑ Attach images

From camera: Camera 2 support - sivu ovi

Limit image size to: Small

Maximum images: 3

Time before alarm: 1s

Time after alarm: 1s

After this, you can choose a camera, size for the image scaling, desired number of images, and the time span from which the images are fetched.

Note:

- The number of images in this configuration is the maximum amount delivered. Fewer images might arrive
- Attaching images to alarm emails might lead to high data traffic, so it is recommended to test the configuration settings to find the optimum setting.

- If you experience issues that no images are arriving with the default settings, it is recommended to select more than one image to the “maximum images” setting and adjust the sliders slightly to have a longer duration of time where the images are being fetched.

The action includes the following fields and parameters:

Format – Defines the message format as short or usual.

- A short message will contain only up to 160 characters and cannot contain additional message text or image attachments (see below).

Message – This field contains the message that will be sent to the recipients if the alarm occurs. The message field is active only if the e-mail format has been set as long.

Note:

- *Unlike other alarm actions, the **Send e-mail** action can be selected only once for each alarm. Once selected, the action will disappear from the list of available actions.*
- The message will have the alarm name in the title.

Disable Alarms

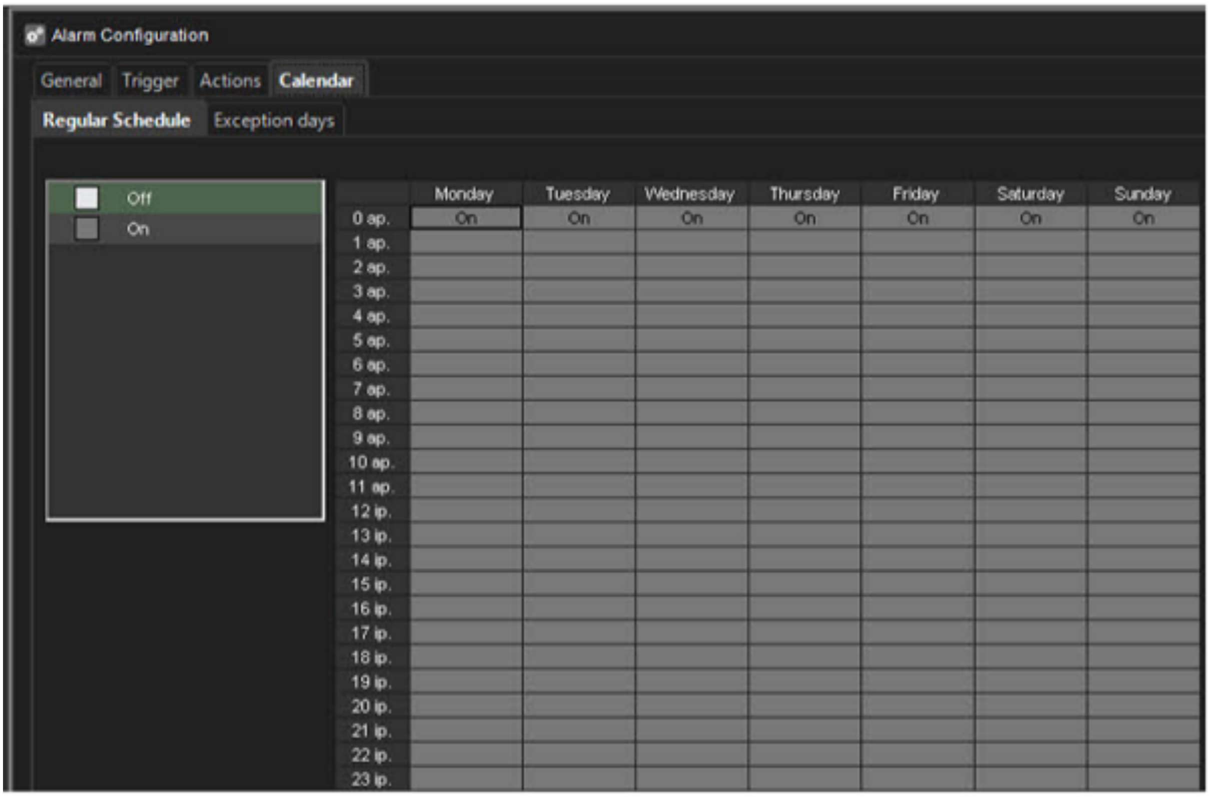
The **Disable alarms** action can be used to send disable alarms based on one alarm. The configuration can be done so that all alarms are disabled, low and medium priority alarms, or low alarms.

This option allows specific alarms to remain active while others are suppressed.

The alarms are disabled only while the alarm that disables them is active.

Calendar

- Define that when the alarm is active
- Click **OK**



Alarm Configuration

General | Trigger | Actions | **Calendar**

Regular Schedule | Exception days

□ Off
■ On

	Monday	Tuesday	Wednesday	Thursday	Friday	Saturday	Sunday
0 ap.	On	On	On	On	On	On	On
1 ap.							
2 ap.							
3 ap.							
4 ap.							
5 ap.							
6 ap.							
7 ap.							
8 ap.							
9 ap.							
10 ap.							
11 ap.							
12 ip.							
13 ip.							
14 ip.							
15 ip.							
16 ip.							
17 ip.							
18 ip.							
19 ip.							
20 ip.							
21 ip.							
22 ip.							
23 ip.							

Holiday Schedules

Alarm specific holiday schedules can create schedules for specific dates or set a specific date to use an alarm schedule designed for another weekday. The **Holidays** sub-tab can be accessed through the alarm's **Schedule** tab.

To set a specific date to function with another weekday's schedule:

- Select the weekday from the schedule list on the left side of the screen.
- Select the desired year and month from the drop-down menus above the calendar.
- Click on a date in the calendar to add the schedule.

To create a custom schedule:

- Click Add at the upper left side of the screen.

- Type the name of the holiday schedule in the **Schedule name** field.
- To create the schedule, select **Off** from the **On/Off** list on the left side of the screen and mark the hours the alarm is switched off for the day.
- Click **OK** to save the schedule.
- Select the desired year and month from the drop-down menus above the calendar.
- Click on a date in the calendar to add the schedule.

To edit a custom schedule:

1. Select the custom schedule from the schedule list on the left side of the screen.
2. Click **Edit** at the upper left side of the screen.
3. Edit the schedule.
4. Click **OK** to save the changes.

To delete a custom schedule:

- Select the custom schedule from the schedule list on the left side of the screen.
- Click **Remove** at the upper left side of the screen.

To restore the original schedule:

1. Click **Restore** in the schedule list on the left side of the screen.
2. On the calendar, click the day that you want to restore.

Deleting an Alarm

To delete an alarm:

1. On the **VMS Servers** tab, select the server.
2. Double-click on **Alarms**.
3. Select the alarm you want to delete by clicking on its name.
4. Click **Remove Alarm** at the lower-left corner of the **Alarms** screen.

5. The alarm is deleted from the system.

Storage

In storage settings, you can set the storage time of the recorded video, audio and text data, and alarm data.

In addition, after adding a hard disk to a server, you can set it as additional data storage through the storage settings.

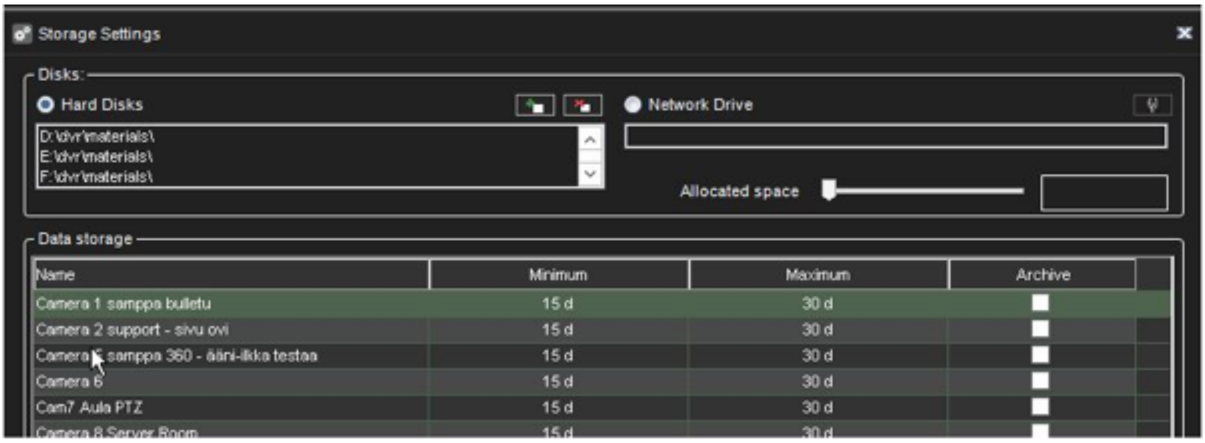
The storage settings are also used to configure the automatic archiving functionality, enabling the creation of backup copies of the server-specific video, audio, and text data daily or weekly.

Video, audio, text data, and alarm recordings are kept until their defined **Maximum** date has been exceeded or until the allocated storage space has run out.

Adding Storage Space

If additional storage space is required, you can add new hard disks or map a network drive for data storage (i.e., NAS support).

There can be multiple network storage disks, and local disks used simultaneously, as seen in the picture.



D:\dvr\materials\
E:\dvr\materials\
F:\dvr\materials\

Name	Minimum	Maximum	Archive
Camera 1 samppa bulletu	15 d	30 d	□
Camera 2 support - sivu ovi	15 d	30 d	□
Camera 5 samppa 360 - ääni-ilkka testaa	15 d	30 d	□
Camera 6	15 d	30 d	□
Cam7 Aula PTZ	15 d	30 d	□
Camera 8 Server Room	15 d	30 d	□

Note: *When adding storage drives to legacy Mirasys filesystem (VMS server version 7.5.x or earlier), the storage drives are recommended to be all of the same capacity, and any single disk should be less than 10TB in size, and the total amount per VMS server should be less than 25 TB in size.*

The use of multiple storage disks has the benefit of allowing material write to be distributed to all the drives, making a loss of any single material drive less likely to wipe out large parts of the stored material.

To add a hard disk:

1. Install the new disk.
2. In Storage Settings, click **Add Disk**.

3. The Add Disk dialogue box is shown. The Minimum free space on the new disk box shows how much free space the new disk must-have.
4. Select the disk from the list and click **OK**.

To map a network drive:

1. In **Storage Settings**, mark the **Network drive** checkbox.
2. If needed, click **Define network drive** to open the network drive configuration screen.

3. Type the network drive username and password into the **Username** and **Password** fields.
4. Type the location of the network drive into the **Network drive path** field.
5. Click **OK**.
6. Use the **Allocated space** slider to set the space reserved on the network drive for data storage.

To map multiple network drives:

- Install and configure the networks storage to work as a locally mapped drive (for example, use iSCSI initiator or similar).
- In Storage Settings, click **Add Disk**.

The Add Disk dialogue box is shown.

- Storage size cannot be configured for iSCSI disks.
- Click ok to store settings. Repeat for other disks.

Video, audio and text data storage settings

Minimum

To prioritize recordings from one or more video, audio or text data channels, ensure that the minimum values are sufficiently low for other channels.

Then set the value higher for the high priority channel or channels.

If you select **Automatic**, the system deletes recordings from channels that use the most storage space.

Maximum

The system examines the recordings daily and deletes those that are older than the maximum number of days.

If you select **Automatic**, the recordings will be deleted only when the free space is not sufficient.

Note*: If the minimum values are too high for some channels while, at the same time, they are not set for other channels, the system will delete recordings from the channels with no set minimum.*

Alarm limits

Minimum

The system deletes alarms that are older than the minimum value.

If you select **Automatic**, the system deletes alarm recordings from channels that use the most storage space.

Maximum

The system examines the alarm recordings daily and deletes them older than the maximum number of days.

If you select **Automatic**, the recordings will be deleted only when the free space is not sufficient.

Log entries

This value specifies how many alarm events will be kept in the alarm log at the most.

The system examines the number of log entries hourly and deletes the oldest entries if they are exceeded.

% maximum

This value specifies how much storage space alarm recordings are allowed to use of all storage space.

As long as all storage space is not used, alarm recordings can use more space than this value.

The system first deletes the oldest alarm recordings before deleting other video or audio recordings if all storage space is used.

Automatic Deletion of Video, Audio and Text Data

After exceeding the defined maximum storage time, stored video, audio, text, and alarm data is automatically deleted—the maximum storage time for data the system checks daily.

As the size of a stored data stream can vary significantly due to movement in the video image, changes in audio levels, or the number of text data events, it may be hard to predict storage space requirements accurately.

Thus, sometimes the system may deem it necessary to ensure free storage space by automatically deleting old material regardless of the maximum storage time.

If data needs to be deleted to ensure free storage space, the deletion process proceeds through the following pattern:

In simple words this retention process goes like this when FS need a new free file:

1. Check alarm quota, if alarm material files count in more then set in quota (% from all data) we cleanup oldest alarm file and reuse it
2. Check min settings for alarm data - if alarm channels have data that exceed min alarm settings – we take the oldest file from those, cleanup it and reuse
3. Check min settings for all material channels (video, audio, data) - if some channels have data that exceed min settings – we take the oldest file from those, cleanup it and reuse
4. Check the oldest file from channels with auto min settings if they are present, if so - we take the oldest file from those, cleanup it and reuse
5. If still, nothing is found – we just take the oldest file from all channels (material and alarm), clean up it and reuse

Also, we have a background task that cleans up material files according to max settings.

The launch period is set to a minimum max setting from all channels (material and alarm).

Note: *To ensure that the need for automatic deletion due to a lack of disk space is minimized, it is good to monitor the disk usage regularly and alter the maximum storage time and allocated disk space.*

It is advisable to use manual or automatic archiving tools to ensure that no relevant data is deleted in storage space issues.

Hint: *You can set a Watchdog event to notify you if the storage space runs low.*

Archiving

You can set the system to automatically archive video, audio, and text data daily or weekly.

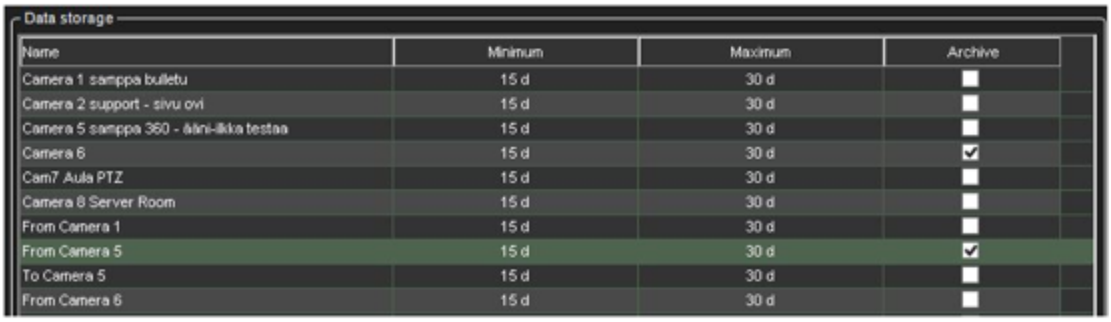
The archive files can be automatically created on the server's hard disks or a network drive.

The archive files can be opened on any Spotter client.

Note: *Archive files can be huge, and thus they can fill storage space quickly. Archive files should be regularly copied and removed from the server hard disks or network drives on which they are automatically saved.*

To set an automatic archiving schedule:

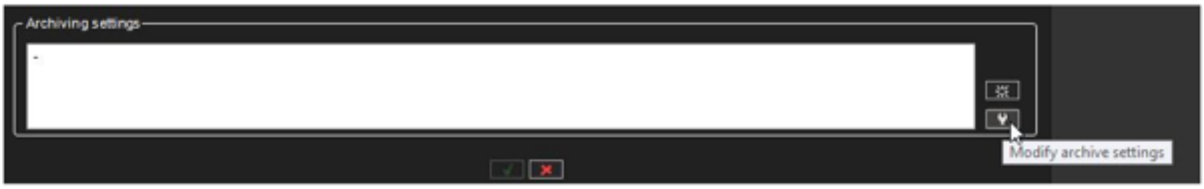
1. In the **Data storage** pane, click on the devices you want to include in the automating archiving process.
   TIP: Select adjacent devices or folders, hold down the SHIFT key and then click the first and last device you want to select.
   a. To add a device to a selection or remove it from a selection, keep the CTRL key pressed and then click the device you want to add or remove.
      Note: *Selecting a device group (folder) also selects its contents.*
2. Mark the **Archive** checkbox.



Data storage

Name	Minimum	Maximum	Archive
Camera 1 samppa bulletu	15 d	30 d	□
Camera 2 support - sivu ovi	15 d	30 d	□
Camera 5 samppa 360 - ääni-ilkka testaa	15 d	30 d	□
Camera 6	15 d	30 d	☑
Cam7 Aula PTZ	15 d	30 d	□
Camera 8 Server Room	15 d	30 d	□
From Camera 1	15 d	30 d	□
From Camera 5	15 d	30 d	☑
To Camera 5	15 d	30 d	□
From Camera 6	15 d	30 d	□

3. Click **Modify archive settings**



4. Set the archive password by clicking **Change archive password**

5. Select whether to create the archive daily or weekly by selecting **Every day or Once a week**

6. If you set archiving to occur daily, use the **Archiving time** drop-down menu to select the time on which the archive files are created.

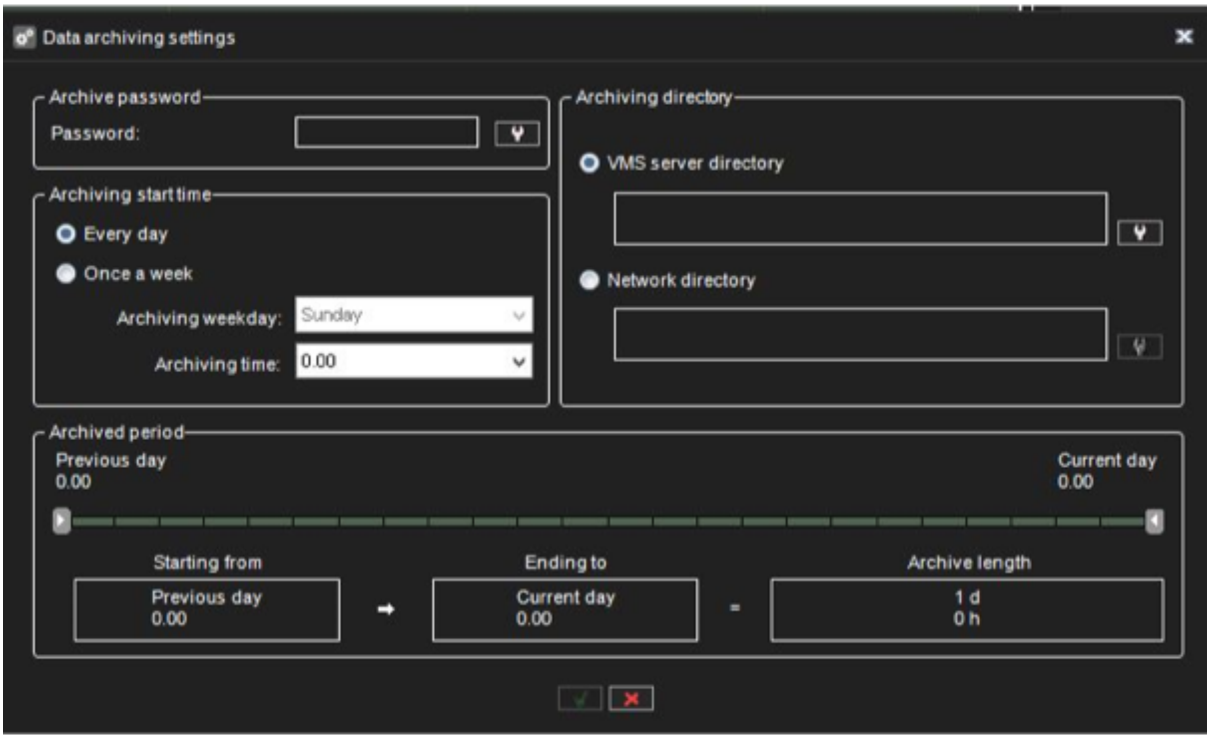
7. If you set archiving to happen every week, use the **Archiving weekday** and **Archiving time** drop-down menus to select the date and time on which the archive files are created.

8. Use the **Archived period** slider to set the period used in the archive files.

9. Select whether to create the archives on a local drive (on the server) or a network drive by selecting the **VMS Server directory** or **Network directory**.

10. Click the **Change directory** or **Change network drive** button to set the directory to save the archives.

11. Click **OK** to set the archiving schedule



Data archiving settings

Archive password

Password:

Archiving start time

● Every day

○ Once a week

Archiving weekday: Sunday

Archiving time: 0.00

Archiving directory

● VMS server directory

○ Network directory

Archived period

Previous day 0.00

Current day 0.00

Starting from		Ending to		Archive length
Previous day 0.00	➡	Current day 0.00	=	1 d 0 h

✓ ✕

Use OS cache

DVMS 8. x and newer have the possibility to enable OS cache usage when accessing the physical disk.

DVMS 9.4 and newer have the possibility to set maximum OS cache size.

Any software can access the disk in direct access mode when OS doesn't use any caching and using OS cache.

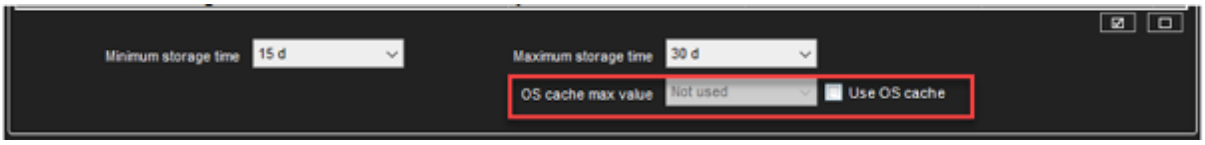
The last one helps to deal with unstable load to HDD and caching most used parts of data.

Windows Server and Windows desktop versions have different priorities for applications - Windows Service priorities background services and desktop version priorities UI applications.

Also, Windows Server uses more system resources to cache e.g. HDD access and can use up to 90% of RAM for this.

To avoid situations when all RAM is occupied by file system cache DVMS 9.4 and newer has an option to limit max OS cache size.

Max OS cache setting is valid until PC reboot, so they are set each time recorder starts.



Minimum storage time: 15 d

Maximum storage time: 30 d

OS cache max value: Not used

☐ Use OS cache

Text Channel Settings

The servers can receive text data from devices such as cash registers or gas station pumps.

The driver specifies what text data is recorded and what is shown to the users. It also specifies custom events and searches criteria.

In addition to the default text data drivers included in the software, new drivers can be installed.

In-text channel settings, you can change the name of a text channel and add or edit its description.

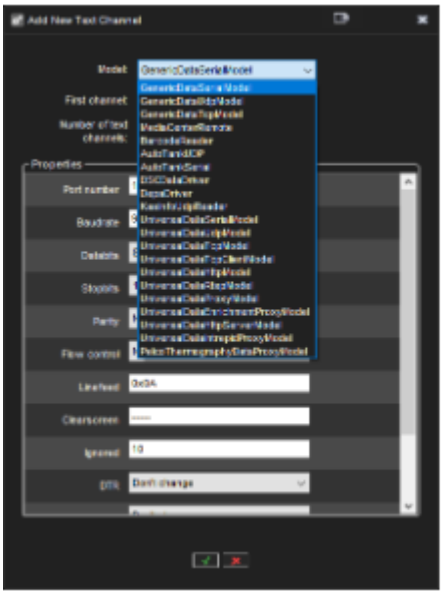
In profile **settings**, you can set the user rights and the device window options for each channel and each profile.

An additional document for UniversalData drivers can be downloaded from our extranet or contact support. This driver opens endless possibilities for integration to 3rd party systems.

To add text data channels:

1. Click **Add channels** in the lower right corner of the **Text channel settings** screen.

2. Select the text data channel driver from the **Model** drop-down menu.



3. Use the **No. of data channels** slider control to select the number of channels you want to create.

4. Fill the driver-specific information into the fields in the **Properties** list.

5. Click **OK** to save the channels.

To edit text channels:

To edit the name and description of a text data channel:

1. Select a text data channel from the channel list.
2. Type a name for the channel into the Name field.
3. Type general and administrative descriptions of the channel into the respective fields.
    a. All users can see the general description, whereas only system administrators can see the administrative description.
4. Mark the **In use** checkbox to set the channel as active, or unmark the checkbox to set the channel as inactive.

To edit the configuration setting of a text data channel:

1. Select a text data channel from the channel list.
2. Click **Modify channels**.
3. Edit the driver-specific information to the fields in the **Properties** list.
4. Click **OK** to save the changes.

Note: *When editing the configuration settings of a text data channel, the settings are changed for all text data channels that use the exact driver.*

To remove all text channels that use the same driver:

1. Select a text data channel from the channel list.
2. Click **Delete channels** in the lower right corner of the **Text channel settings** screen.

3. All text data channels that use the same driver as the selected text data channel are removed.

Note: *To remove text data channels without deleting all channels that use the specific driver, click **Modify channels** and specify the new number of text data channels using the **No. of channels slider**.*

Profiles

Profiles define which VMS components the user has access to and what kind of user rights the user has for the components.

The system has one default profile, Service.

The default profile contains the devices that the license key of the Master Server specifies.

The devices are grouped by device type. For example, all cameras are in one group and all audio channels are in a different group.

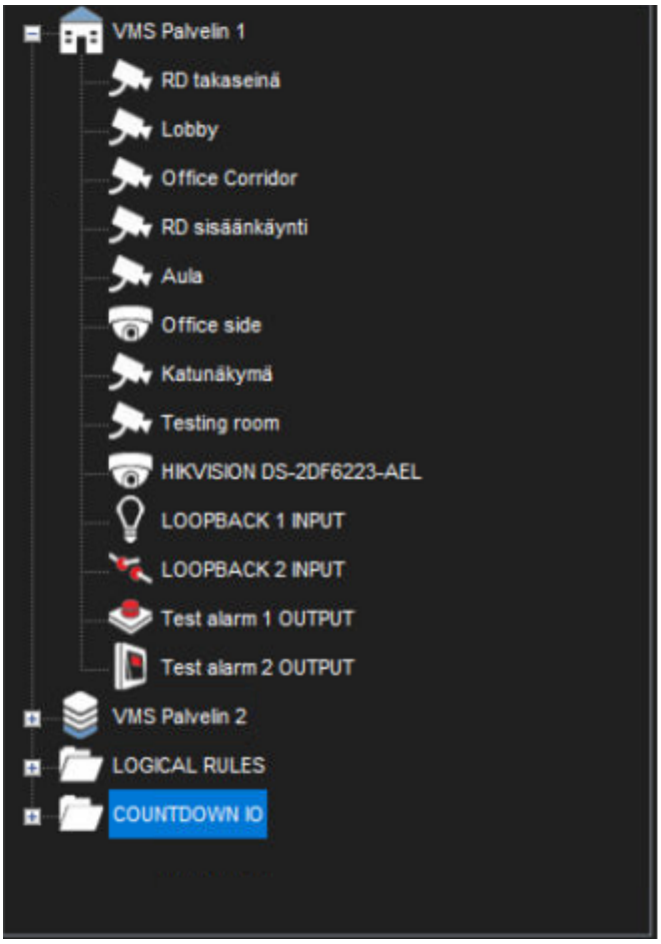
You can use the default profile as such or edit it freely, for example, group cameras at the exact location.

Or you can add new profiles. A profile can contain devices from different servers.

A *profile* sets a user's rights in the system. Each user can have 1 to 5 profiles that contain these *devices*:

1. Cameras (fixed cameras and PTZ cameras)
2. Audio channels
3. Audio communication channel
4. Digital inputs (alarm inputs)
5. Digital outputs (control outputs)
6. Video outputs
7. Text channels
8. Alarms
9. Plugin instances
10. Web browser home pages

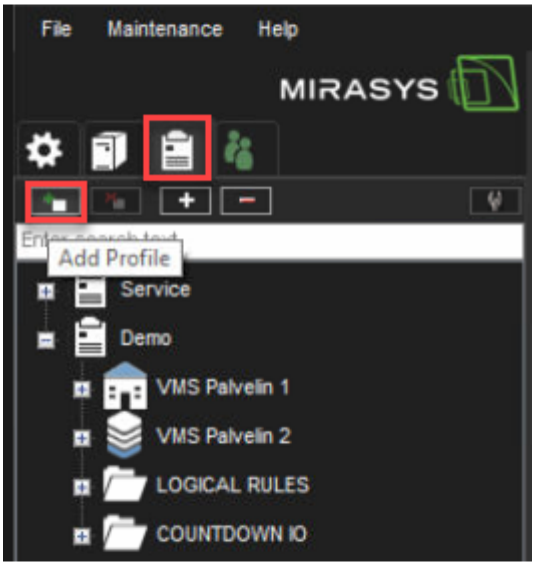
You can add as many as 2,000 groups and devices to a profile. Furthermore, you can put the devices into groups as you like.



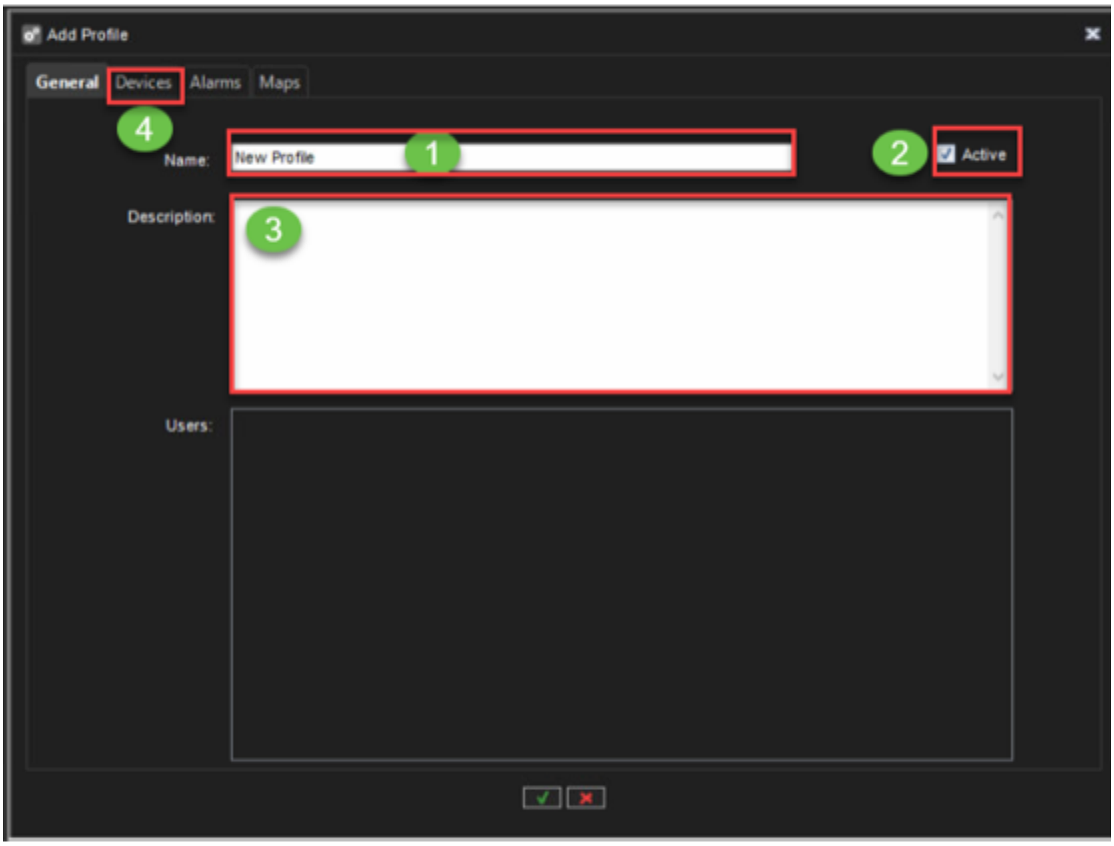
Creating a customer-specific profile

To add a profile:

1. Click **Add Profile**

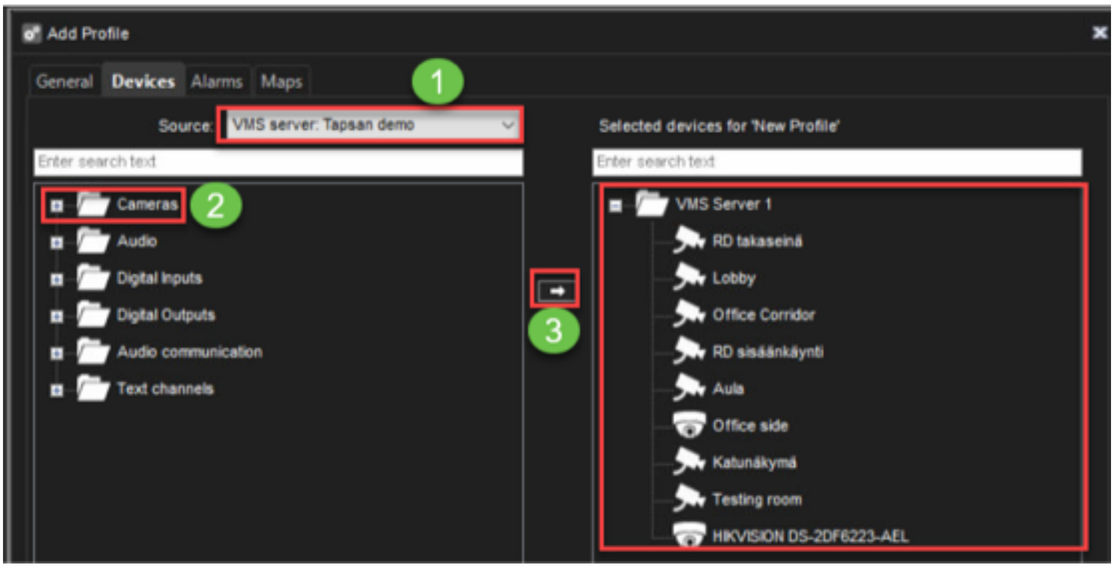


2. Set the name of the profile
3. Set profile status: **Active** or **Disabled**
4. Set description, if needed. The description is shown only in System Manager
5. Open **Devices**



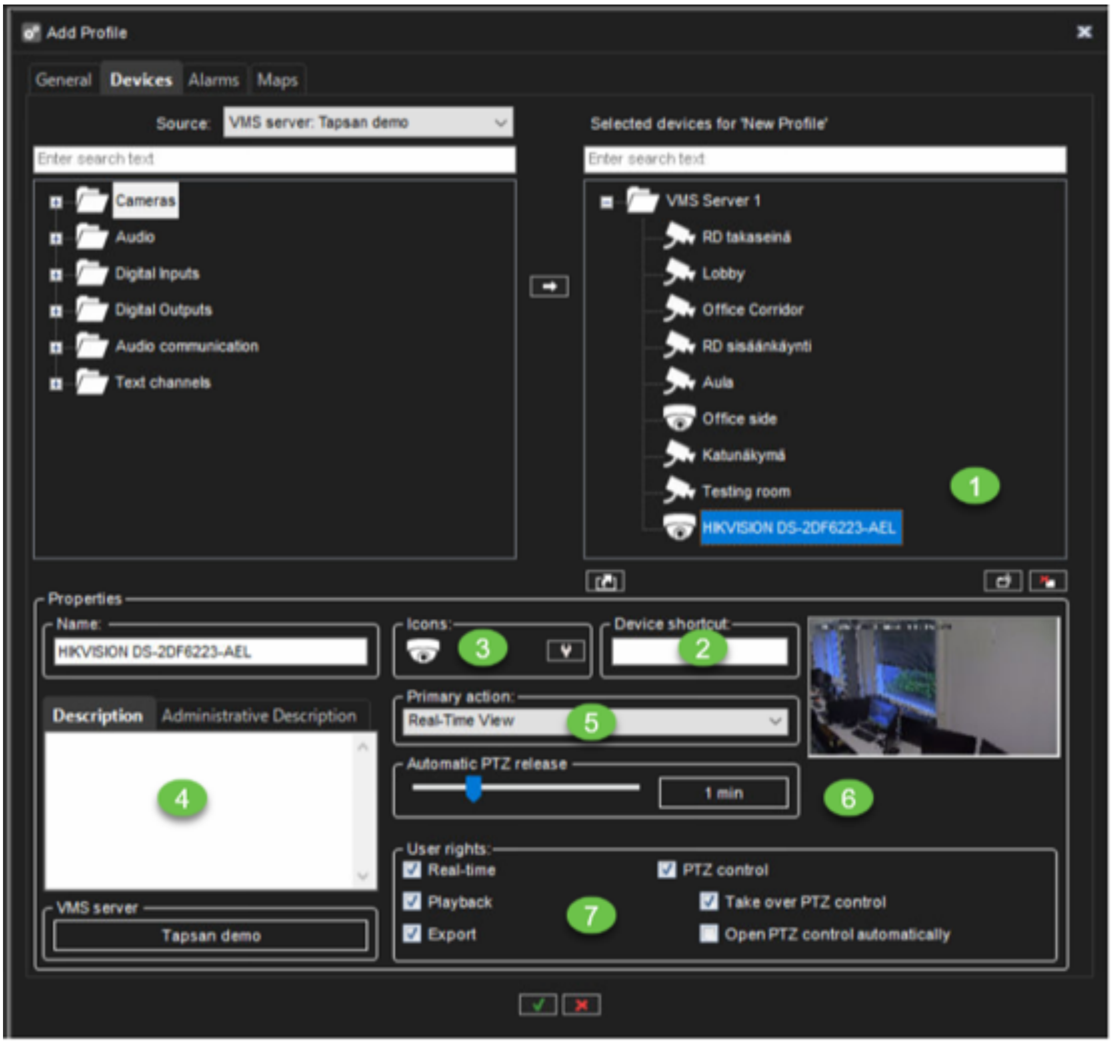
Devices

1. From the Source drop-down list select **VMS server or another profile**
2. Select needed components or device groups from the left box
3. Click **Add**
4. To change selected components properties, please go to **Selected Devices**



Selected Device Properties

1. Select component from the list of the selected device
2. Set **Device shortcut**
3. Change the device icon by clicking **Change Icon**
4. Set **Description** and **Administrative Description**, if needed
5. Select the **Primary action**, select the action that will occur when a user double-clicks the device in Spotter.
6. Set **Automatic PTZ release**(only for the PTZ cameras)
7. Set user rights for the component
    a. **Real-time**
    b. **Playback**
    c. **Export**
    d. **PTZ Control**(only for the PTZ cameras)
        i. **Take over PTZ control**
        ii. **Open PTZ control automatically**
8. Click **OK** to finalize the profile creation



Add Profile

General | **Devices** | Alarms | Maps

Source: VMS server: Tapsan demo

Enter search text

- Cameras
- Audio
- Digital Inputs
- Digital Outputs
- Audio communication
- Text channels

Selected devices for 'New Profile'

Enter search text

- VMS Server 1
  - RD takaseinä
  - Lobby
  - Office Corridor
  - RD sisäänkäynti
  - Aula
  - Office side
  - Katunäkymä
  - Testing room
  - HIKVISION DS-2DF6223-AEL

Properties

Name: HIKVISION DS-2DF6223-AEL

Icons:

Device shortcut:

Description | Administrative Description

VMS server: Tapsan demo

Primary action: Real-Time View

Automatic PTZ release: 1 min

User rights:

☑ Real-time
☑ Playback
☑ Export
☑ PTZ control
☑ Take over PTZ control
☐ Open PTZ control automatically

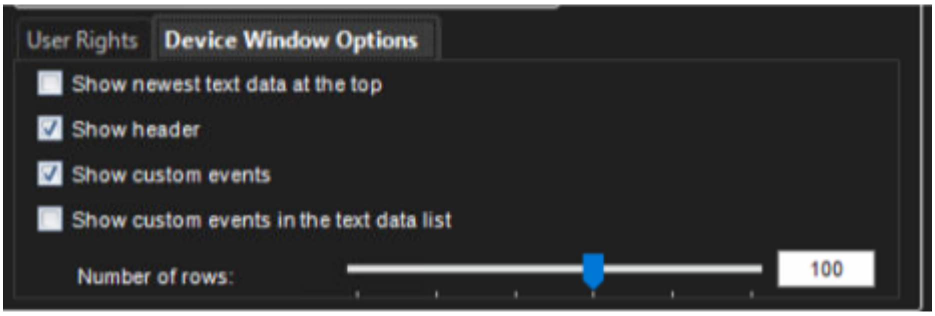
PTZ control

- Automatic dome release
  a. Values: 10s, 20s, 30s, 40s, 50s 1 min, 2 min, 3 min, 4 min, 5 min, 10 min, 20 min, 30 min
- Take over PTZ control
  - No warning popup
- Open PTZ control automatically

Sort selected device nodes

Alphanumeric sorting (a -> z) of selected folder profile nodes is executed when pressing sort button, second press will execute reverse sorting (z -> a,).

Text channel Device Window Options



□ Show newest text data at the top

☑ Show header

☑ Show custom events

□ Show custom events in the text data list

Number of rows: 100

In Device Window Options, you can select how text data is shown to users. These options are available:

Show the newest text data at the top.

By default, the newest text data is added to the bottom of the text data list. Select this option to show the newest text data at the top of the text data list instead.

Show header

Select to show identification data specified by the text data capture driver.

Show custom events

Select to show custom events specified by the text data capture driver.

Show custom events in the text data list

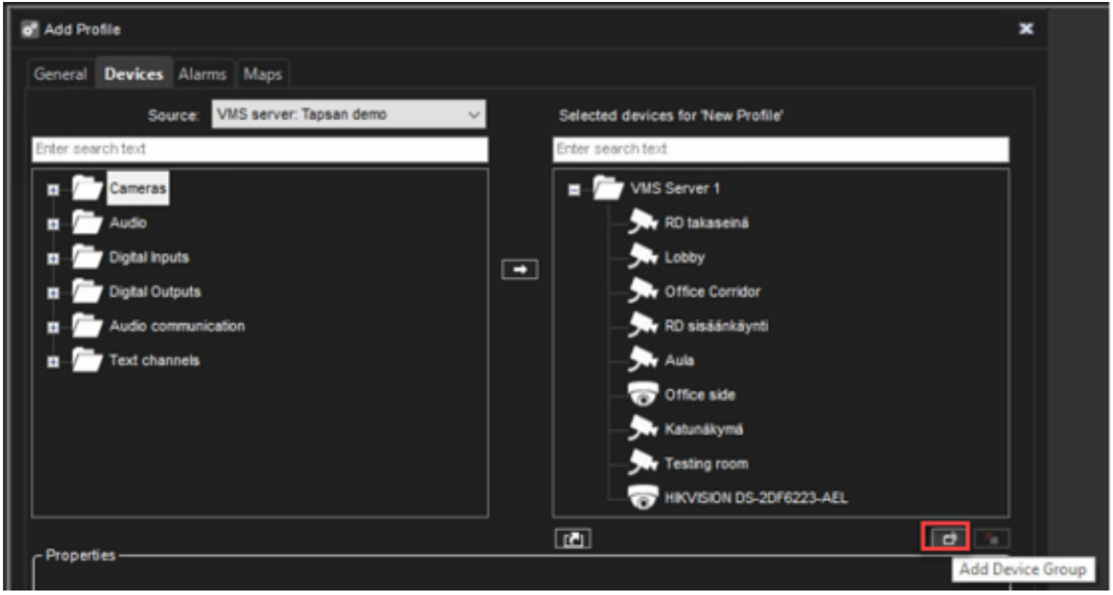
Select to show custom events in the text data list (instead of the custom event list).

The number of rows

Specify the number of rows that are shown in the text data list at the most.

Adding Device Groups to the list of the selected device

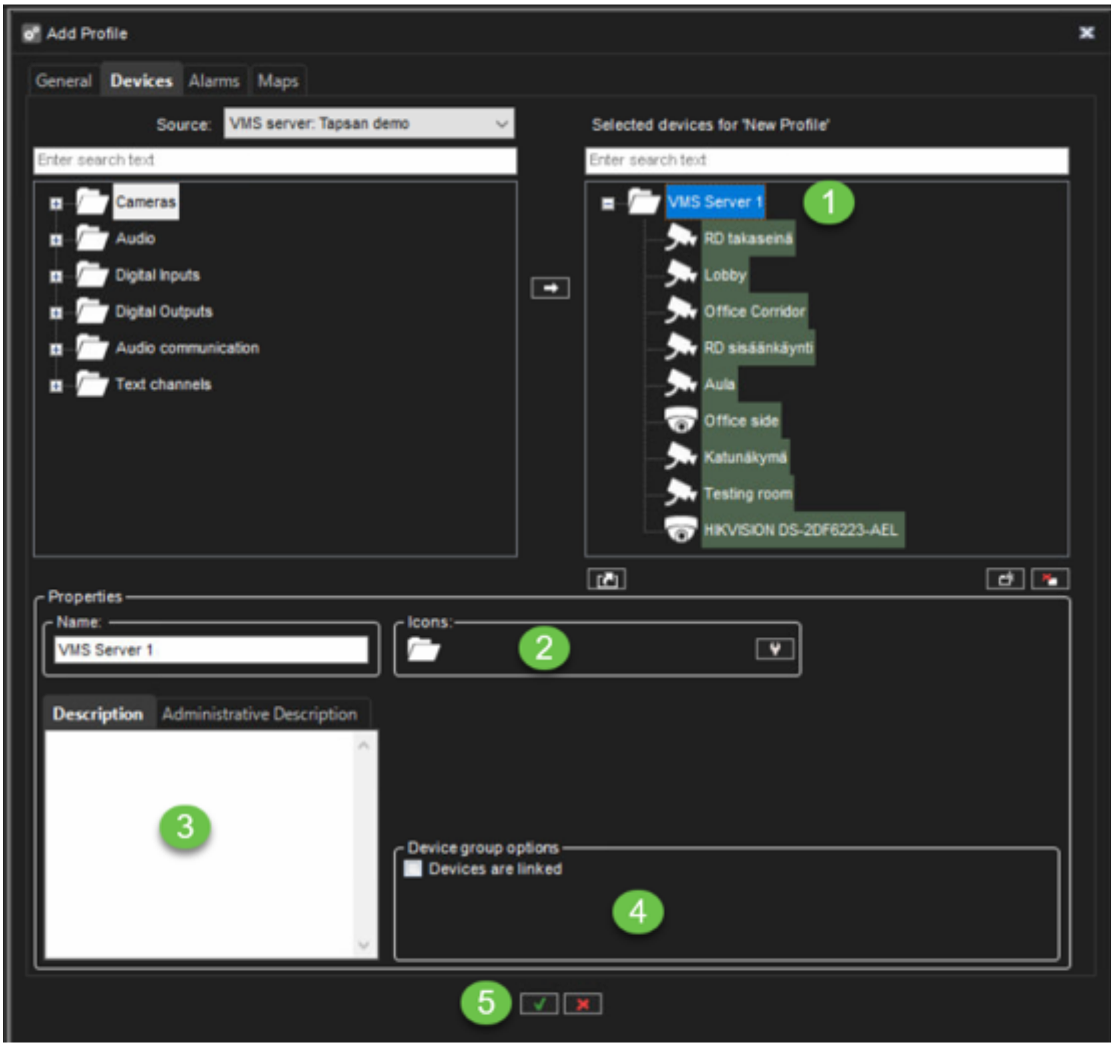
1. Click **Add Device Group** below the **Selected devices** panel. A new device group is shown.



Source: VMS server: Tapsan demo

Note: *A new device group is always added under the selected device group. To add a device group to the top level, make sure that none of the existing device groups is selected.*

1. Click the device group and type a name for it
2. To change the icon that is used for the device group, click **Change Icon**. Then select the icon that you want to use.
3. Type a description of the device group in **Description**.
4. Set Device group options, if needed(**Devices are linked** to automatically open all device views from the same group when the user opens one of the device views).



Sort Alphabetically

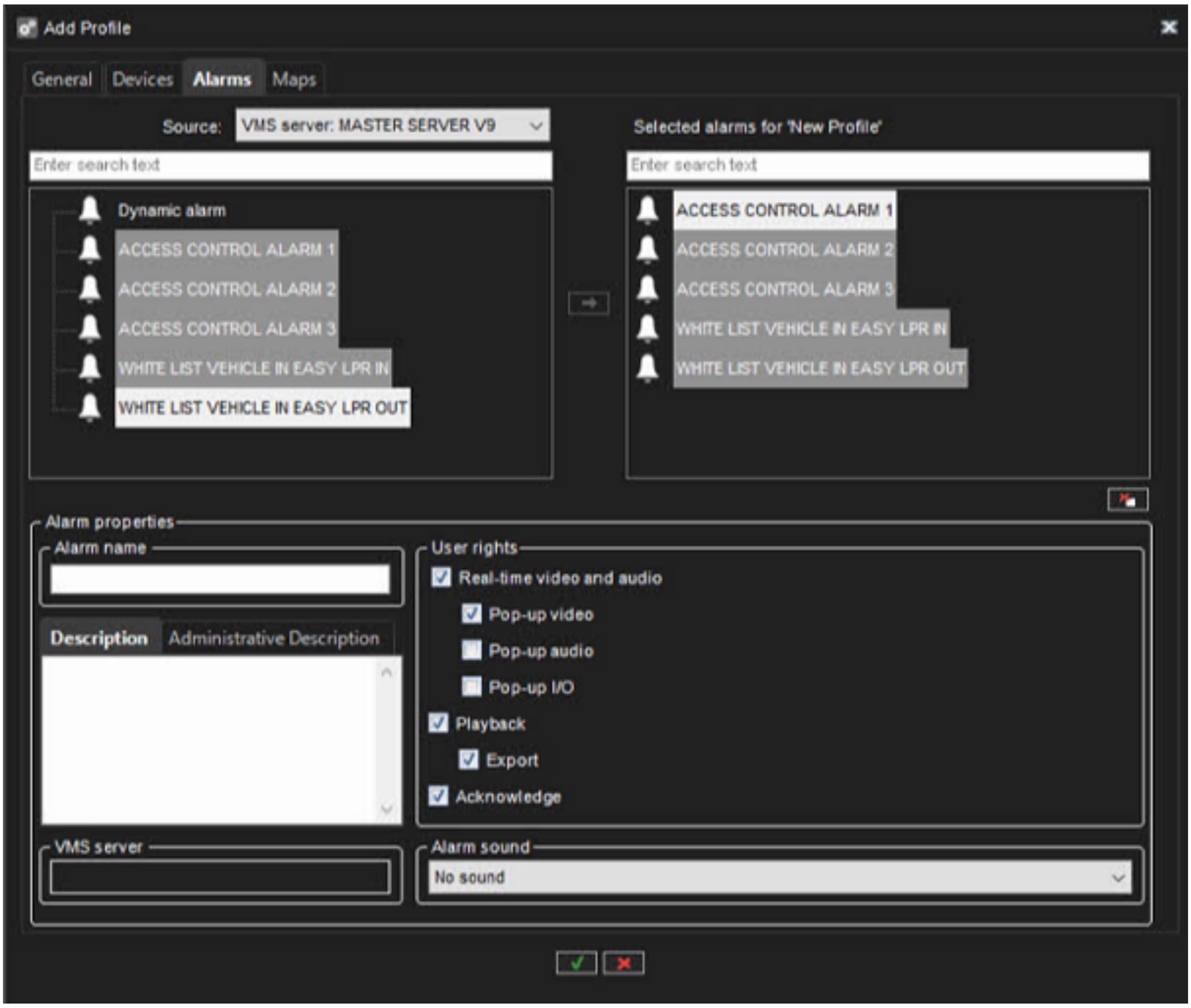
Sorting rules:

- to the folder or root level where the currently selected component is located (but not to subfolders)
- to the selected folders (but nor to subfolders)
- if no profile node is selected, root nodes are sorted (but nor subfolders)

- if multiple folders are selected from same level, all selected folders are sorted (but not subfolders)

Alarms

Editing Profile Specific Alarm Settings



Source: VMS server: MASTER SERVER V9

Dynamic alarm
- ACCESS CONTROL ALARM 1
- ACCESS CONTROL ALARM 2
- ACCESS CONTROL ALARM 3
- WHITE LIST VEHICLE IN EASY LPR IN
- WHITE LIST VEHICLE IN EASY LPR OUT

Selected alarms for 'New Profile'
- ACCESS CONTROL ALARM 1
- ACCESS CONTROL ALARM 2
- ACCESS CONTROL ALARM 3
- WHITE LIST VEHICLE IN EASY LPR IN
- WHITE LIST VEHICLE IN EASY LPR OUT

User rights
- ☑ Real-time video and audio
  - ☑ Pop-up video
  - □ Pop-up audio
  - □ Pop-up I/O
- ☑ Playback
  - ☑ Export
- ☑ Acknowledge

Alarm sound: No sound

On the **Alarms** tab, you can select the alarms you want to include in a profile and edit the alarms' profile-specific user rights.

To add alarms to a profile:

- Open the **Alarms** tab.
- Select a server from the **Source** drop-down menu. The available alarms are shown in the left pane.
- Select the alarm or alarms that you want to add and then click the right arrow. You can also drag alarms from the left pane to the right.
- Save the profile by clicking **OK**.

Note: *You can also add alarms to profiles through the alarm creation/editing screen.*

To edit profile-specific alarm user rights:

1. Open the **Alarms** tab.
2. Click on an alarm in the **Selected alarms** pane.
3. Set the user rights for each alarm. The user rights settings are located on the bottom right side of the **Alarms** tab.
    a. You can set individual rights for each alarm or select multiple alarms (by holding the shift or control keys down while selecting alarms) and set the same options for multiple alarms.
4. To have the computer play a sound when an alarm occurs, select **Alarm sound** and then select the played sound. To test the sounds, select the sound from the list and click **Play**.
5. Save the settings by clicking **OK**.

The user rights include:

- **Real-time video and audio**. Select to let the users see real-time alarm video or audio.
- **Pop-up video**. Select to let users receive alarm video automatically.
- **Pop-up audio**. Select to let users receive alarm audio automatically.
- **Playback**. Select to let the user's playback alarm video.
- **Export**. Select to let the users save alarm video on local media.
- **Acknowledge**. Select to let the users acknowledge alarms.

Maps

Adding Maps to Profiles

To add a map:

1. Click the **Change Level** button and then select the device group to which you want to attach a map. The devices that belong to the selected group are shown in the left pane.
    a. Subgroups are also shown. You can also double-click the subgroup icons in the left pane to move to a lower level.

2. Click **Add Map** and find the image that you want to use as a map.
3. Select the devices and device groups you want to add to the map from the left pane and click the **Add to Map** arrow.
   - Items that are already on the map appear dimmed in the left pane. If you add subgroup icons to the map, the icons will act as links to the subgroup maps.
   - Users can move to a lower level map by double-clicking the subgroup icon.

Tip: To select more than one device simultaneously, keep the SHIFT or CTRL key pressed.

- Select a device or device group from the map, and then, under **Device properties,** you can set these options:
- For cameras, you can select the direction that the camera icon points to.
- By default, the name label of each device is shown on the map. To avoid label clutter, clear the check box **Label**. The name will be shown as a popup label instead.
- If you need to fit several device icons in a small space, you can use placemarks.
- Select the **Placemark** check box. A placemark (x) and a connecting line are shown on the map. Drag the placemark (x) to the device's correct position.
- Then drag the icon to a convenient position on the map.

To remove a site map:

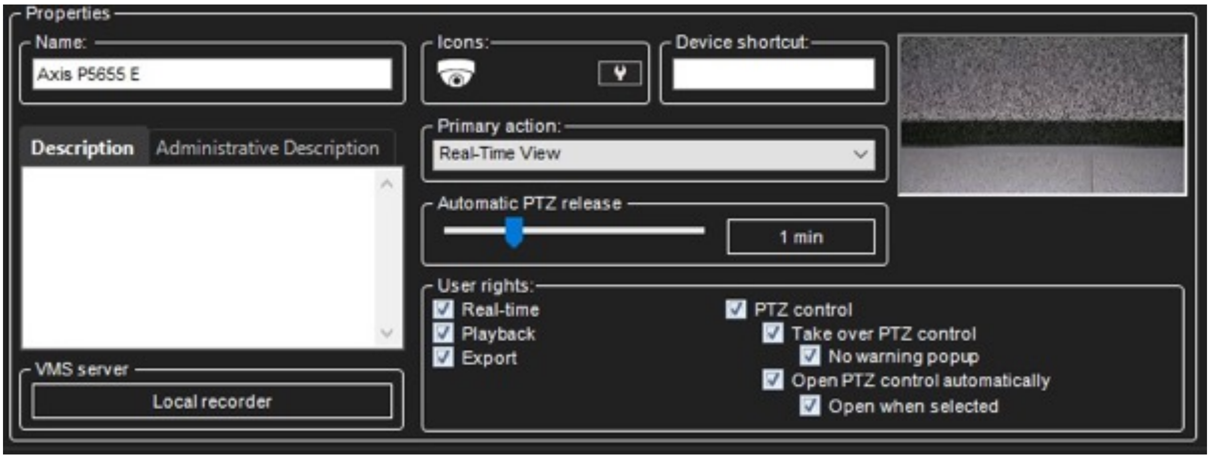
1. Display the map that you want to remove and click **Remove Map**

To remove an icon from the map:

- Select the icon and click **Remove**

PTZ camera profile settings

In System Manager camera profile settings in PTZ camera user rights, selection **Open when selected** is added.



Properties

Name: Axis P5655 E

Icons:

Device shortcut:

Description | Administrative Description

Primary action: Real-Time View

Automatic PTZ release: 1 min

VMS server: Local recorder

User rights:

- ☑ Real-time
- ☑ Playback
- ☑ Export
- ☑ PTZ control
  - ☑ Take over PTZ control
    - ☑ No warning popup
  - ☑ Open PTZ control automatically
    - ☑ Open when selected

If **Open when selected** is selected, then PTZ camera control is automatically activated when PTZ camera view is selected in Spotter.

Users and User groups

All users belong to a user group (see below), through which their use rights are defined and managed.

The administrator can add new user groups, set varying use rights for the groups, and add users.

The system supports domain-level user rights integration (LDAP), enabling users to be synchronized from domain groups.

Each user group must have at least one profile that sets the user group's devices in the system.

One user group can have five profiles at the most.

A username and a password protect all user accounts.

Logging Users Off

If you have administrative rights, you can log a user off from the Spotter program.

To log a user off:

Right-click the username on the Users tab and click **Log User Off.**

NOTE:

Please change always the Admin user password after you have finalized the installation.

You should never leave default passwords in the Mirasys VMS system.

Monitoring Users

The **Users** tab shows if users are logged on to the system:

Icon	Description
🟩	(Green). The user is logged on. Click the plus sign (+) to see the name of the program the user is logged on to and the IP address of the user’s computer. In addition, the date and time of logon are shown.
🟥	(Red). The user is not logged on.
▨	(Grey) The user account is disabled.

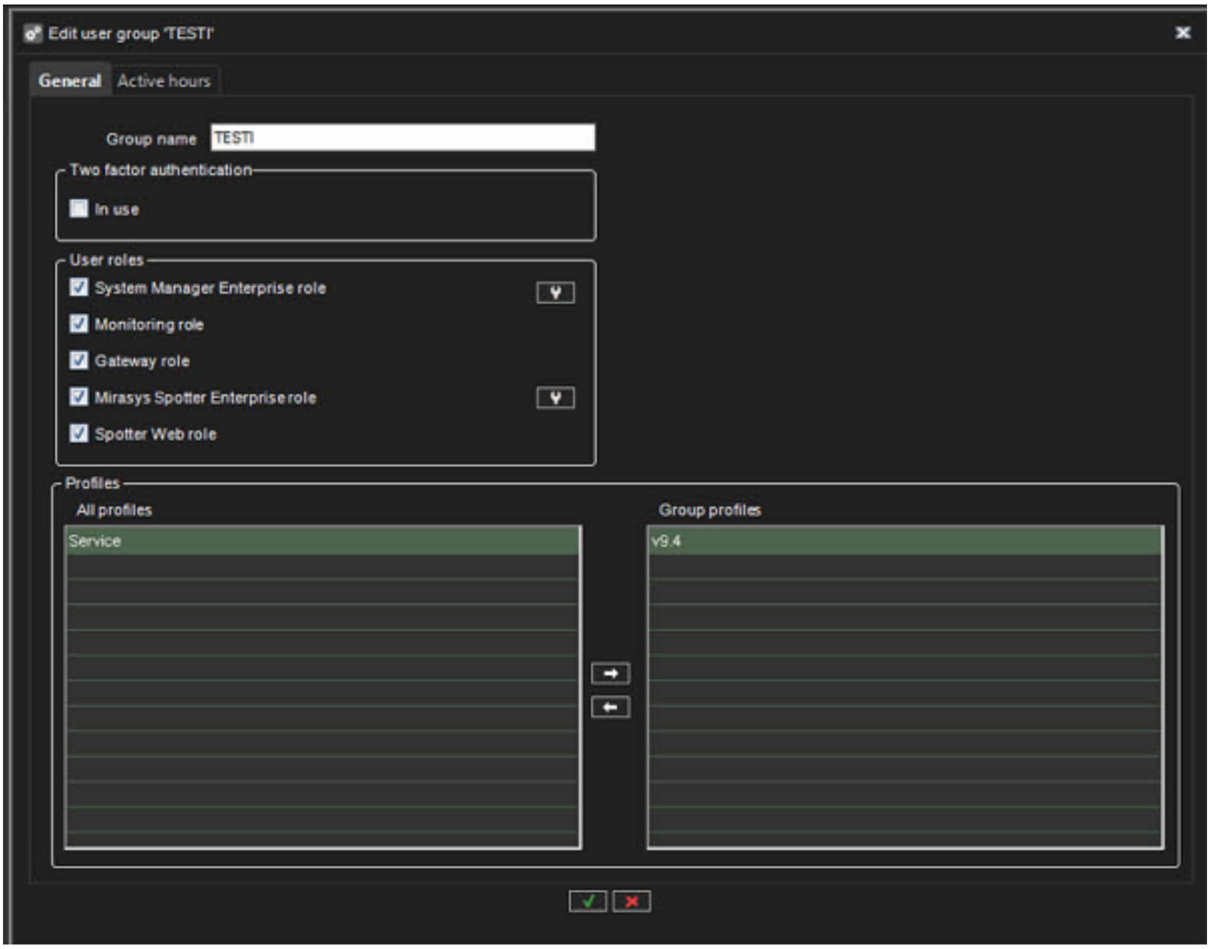
User group

The user group defines which Mirasys VMS applications the user group has access to and what kind of permissions the user group has regarding the applications.

User Roles

The system supports the following types of user roles (defined through user groups)

1. **System Manager role:** Administrators are allowed to log in to System Manager and change all settings, such as changing camera settings or adding new profiles or user accounts.
2. **Monitoring role:** Users with monitoring rights are allowed to log in to System Manager and monitor the system on the **System** tab, but they are not allowed to change the settings.
3. **Gateway role:** if this role is active, the user group can access the DVMS gateway
4. **Mirasys Spotter Enterprise role:** End users can log in to Spotter but not to System Manager.
5. **Spotter Web role:** End users can log in to the Spotter Web


Edit user group 'TESTI'

General | Active hours

Group name: TESTI

Two factor authentication
☐ In use

User roles
☑ System Manager Enterprise role
☑ Monitoring role
☑ Gateway role
☑ Mirasys Spotter Enterprise role
☑ Spotter Web role

Profiles

All profiles	Group profiles
Service	v9.4

User group level automatic lock / log off

Possibility to force other user log off when starting System Manager

- Enabled only if System Manager Enterprise Plus role is enabled
- Possible values for Wait time: 0s, 10s, 20s, 30s, 45s, 1 min
- When creating new group, default value is 10 seconds

Functionality at log on

There is changes from previous versions only if other user log off is enabled and there is other user logged in System Manager with administrator rights.

When trying to log on, following choices will appear:

1. Kick off current user: start sequence to kick off current user with administrator rights in System Manager
2. Login with limited system monitoring rights: continue login with monitoring rights, no effect to current System Manager users
3. Cancel login: go back to start login page (cancel button has this same effect)

Kick off current user

Current user is selected, new processing window is opened:

This processing window is open until:

- Other user is logged off
- Other user has cancelled force log off
- Cancel button is pressed

Other user is logged off

User is automatically logged in with administrator rights.

Other user has cancelled force log off

Other user has cancelled force log off

After OK button, go back to login page, other user with administrator rights continue logged in.

Cancel button is pressed

Go back to login page, other user with administrator rights continue logged in.

Other (already logged with Administrator rights) side

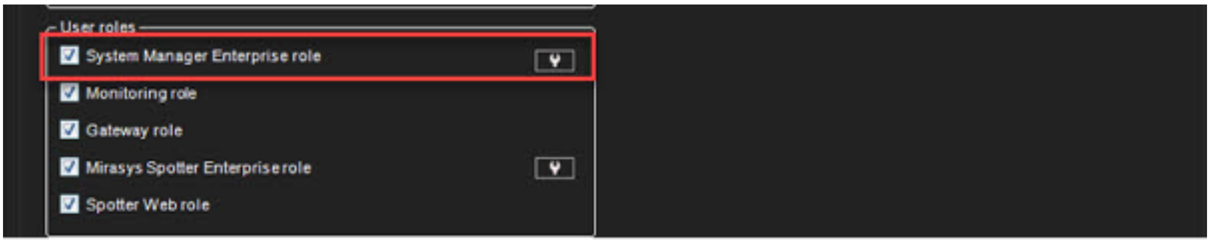
If there is timeout in forced log off settings, warning of coming forced log off appears:

Remaining seconds before forced log off is updated. During this timeout, user can cancel forced log off by cancel button.

If timeout is past or Ok button is pressed, current user session is logged off.

System Manager Enterprise role

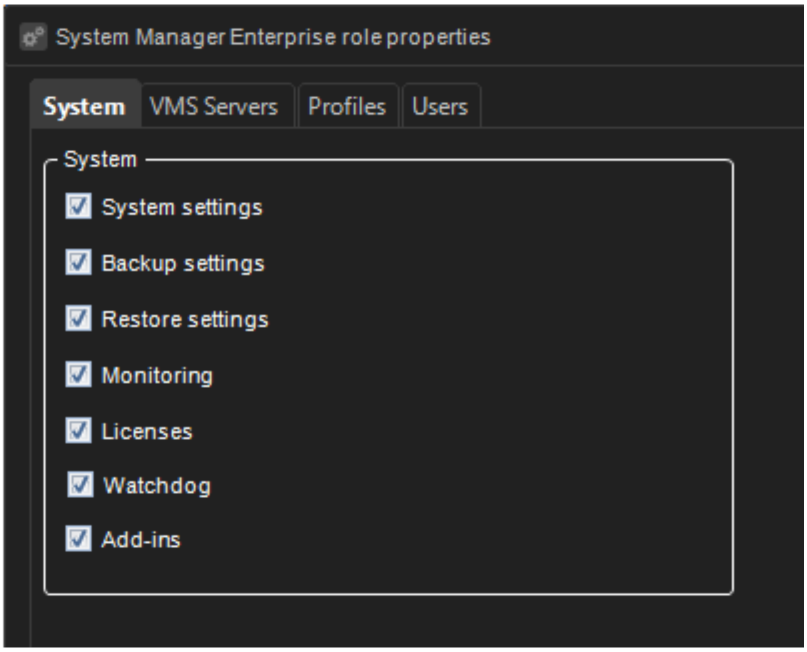
It is possible to set explicit permissions for the system manager for different user groups.
This allows, for instance, implementing functionality for allowing different user groups for hardware maintenance and user administration, which is helpful for large scale systems.
To enable the functionality - check the "System manager enterprise role" tickbox for the user group and click the "wrench" icon to edit the details for this group.



User roles
- ☑ System Manager Enterprise role
- ☑ Monitoring role
- ☑ Gateway role
- ☑ Mirasys Spotter Enterprise role
- ☑ Spotter Web role

System

The System tab permissions can be enabled or disabled for a user group, disabling, for example, System settings hides system settings for all users in the user group



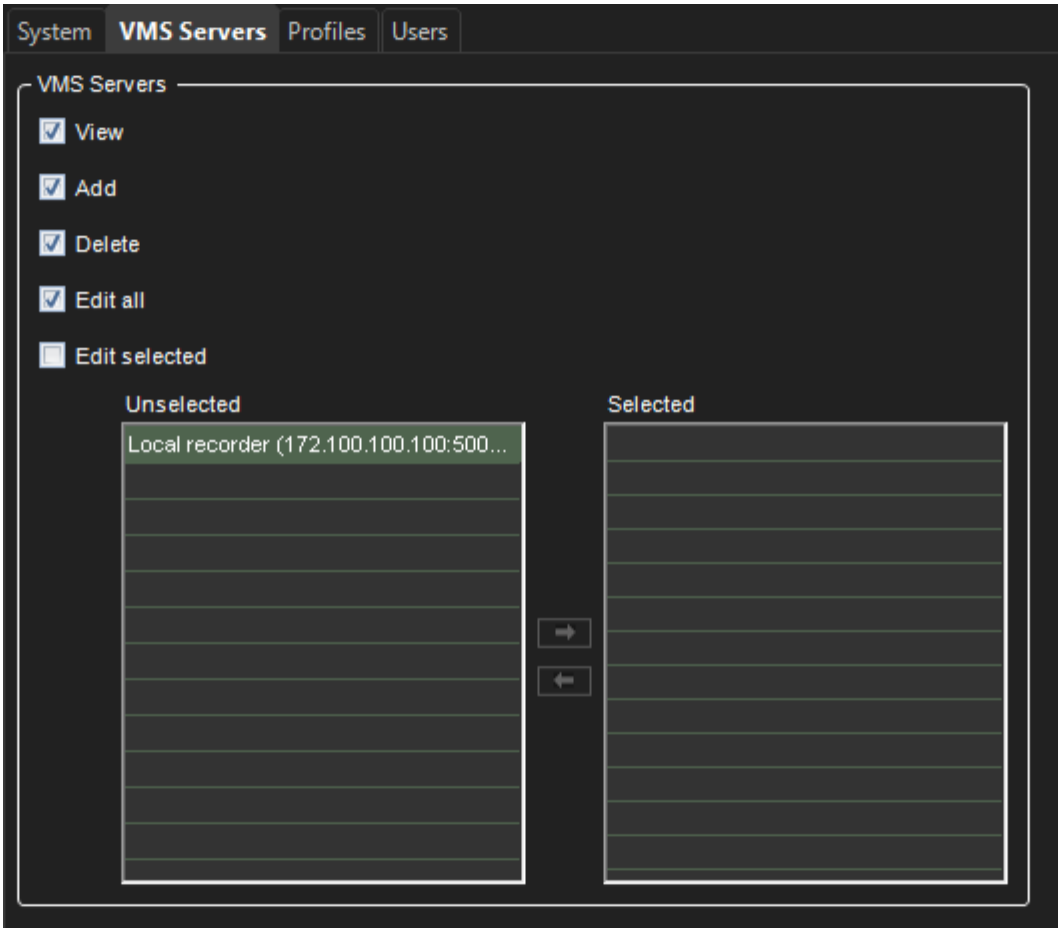
System Manager Enterprise role properties

System
- ☑ System settings
- ☑ Backup settings
- ☑ Restore settings
- ☑ Monitoring
- ☑ Licenses
- ☑ Watchdog
- ☑ Add-ins

VMS Servers

The VMS servers tab allows permissions for a user group to View, Add, Delete and edit either all or only selected VMS Servers to be noted: if "Edit selected" is checked, the shuttle box below enables defining which specific servers this user group has access to.

This is convenient in large installations if specific user groups are working with specific servers (e.g. if there are separate maintenance groups for different sites - and the recording servers are site-specific.)



VMS Servers

☑ View

☑ Add

☑ Delete

☑ Edit all

□ Edit selected

Unselected

Local recorder (172.100.100.100:500...

Selected

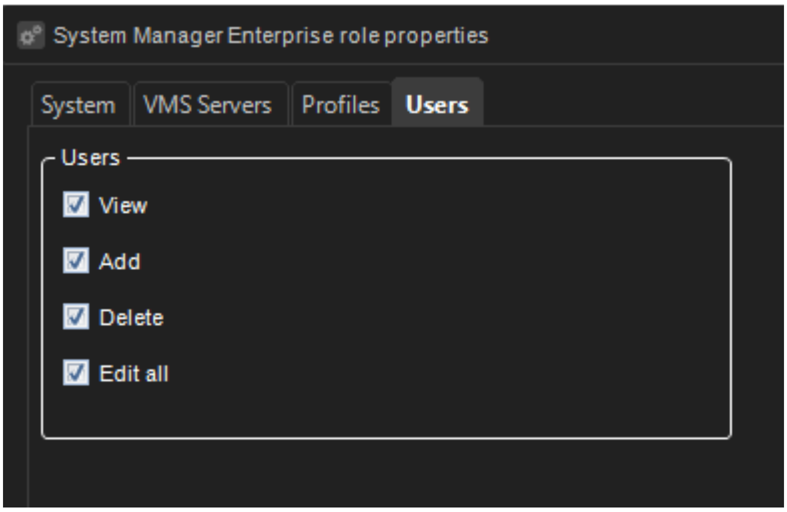
Profiles

The Profiles tab/permissions that can be set for the user group:

“Edit selected” enables you to decide to which profiles the functionality applies (similar to the "servers" permission configuration).

Users

The user tab/permissions that can be set for the user group:



System Manager Enterprise role properties

Users

☑ View

☑ Add

☑ Delete

☑ Edit all

Edit all or Edit selected must be enabled for a user group for users to add and/or delete (these options get automatically disabled if Edit all or Edit selected is disabled).

This functionality affects VMS Servers, Profiles and Users tabs

Monitoring role

The users with the role Monitoring role have permission to:

System

- Export logs

- SM Server and VMS server diagnostic
- Licenses
- Watchdog log

Profiles

Can view the content of the profiles

Users

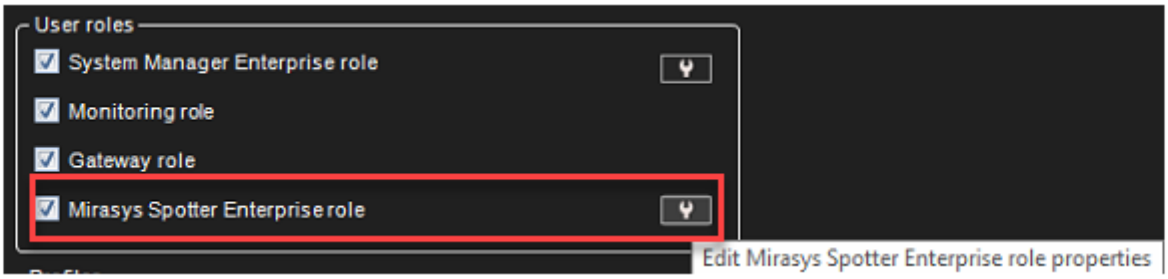
Can view the system user groups and users

Gateway role

Gateway role enables old Spotter Mobile usage

Mirasys Spotter Enterprise role

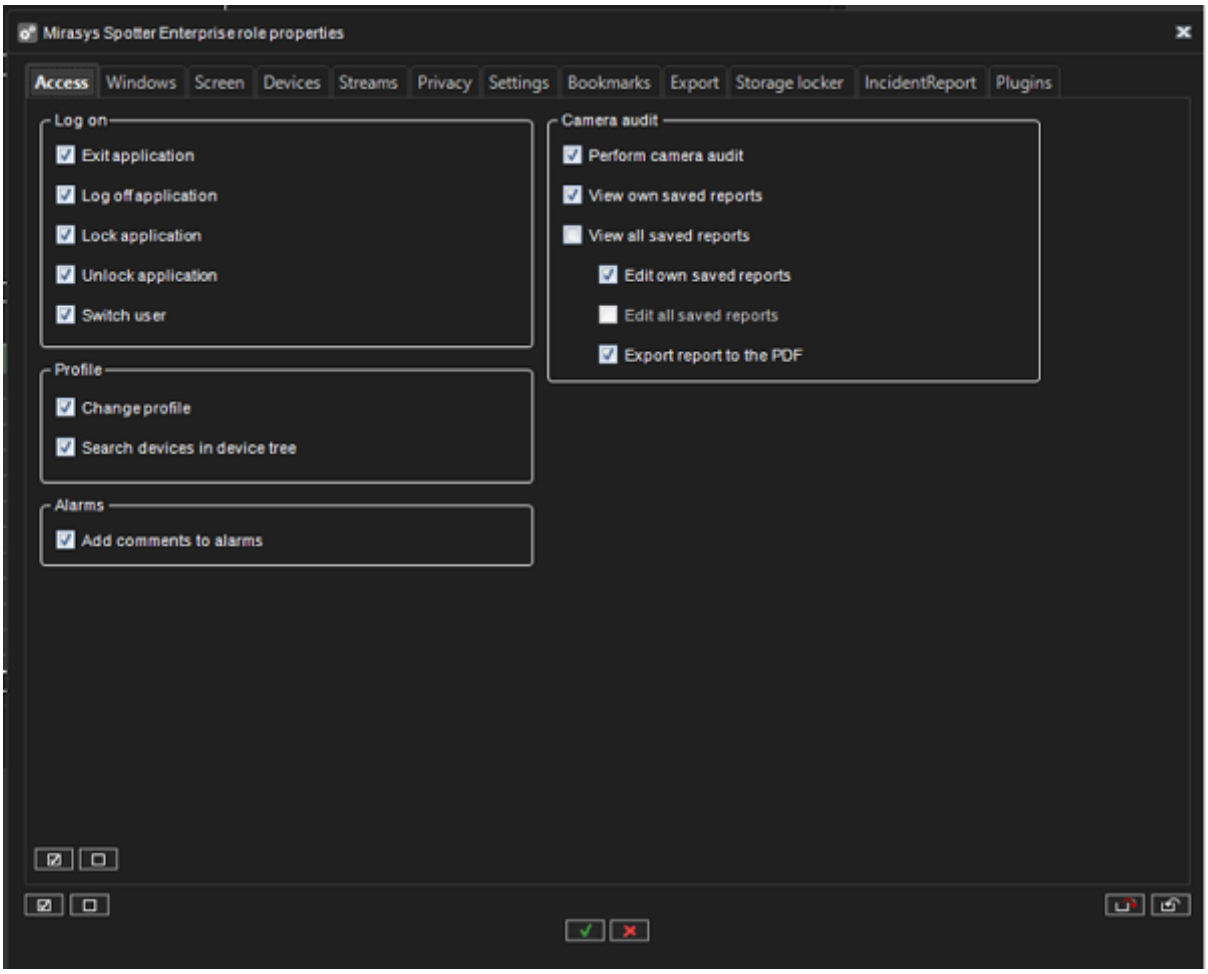
Custom user role properties can be edited by clicking the custom role properties edit button.


User roles
☑ System Manager Enterprise role
☑ Monitoring role
☑ Gateway role
☑ Mirasys Spotter Enterprise role
Edit Mirasys Spotter Enterprise role properties

The **Spotter** custom roles can be customized with close to a hundred different options (not including plugin-specific adjustments).

Access

The Access tab of the role customization contains options for the application access and accessing profiles and alarm commenting.



Mirasys Spotter Enterprise role properties

Log on

- ☑ Exit application
- ☑ Log off application
- ☑ Lock application
- ☑ Unlock application
- ☑ Switch user

Profile

- ☑ Change profile
- ☑ Search devices in device tree

Alarms

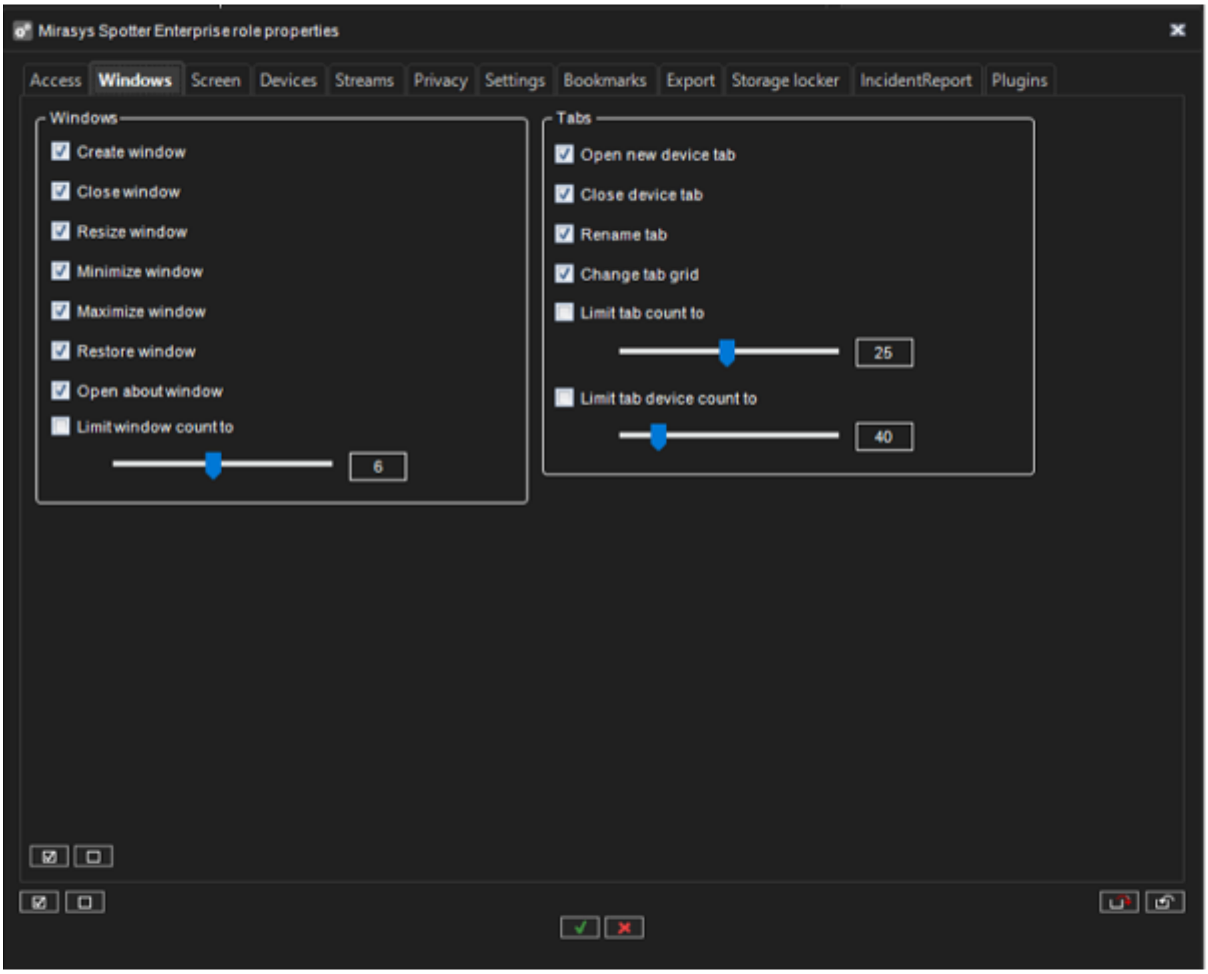
- ☑ Add comments to alarms

Camera audit

- ☑ Perform camera audit
- ☑ View own saved reports
- □ View all saved reports
  - ☑ Edit own saved reports
  - □ Edit all saved reports
  - ☑ Export report to the PDF

Windows

The Windows tab contains options for Spotter window management and tab management.



Mirasys Spotter Enterprise role properties

Windows

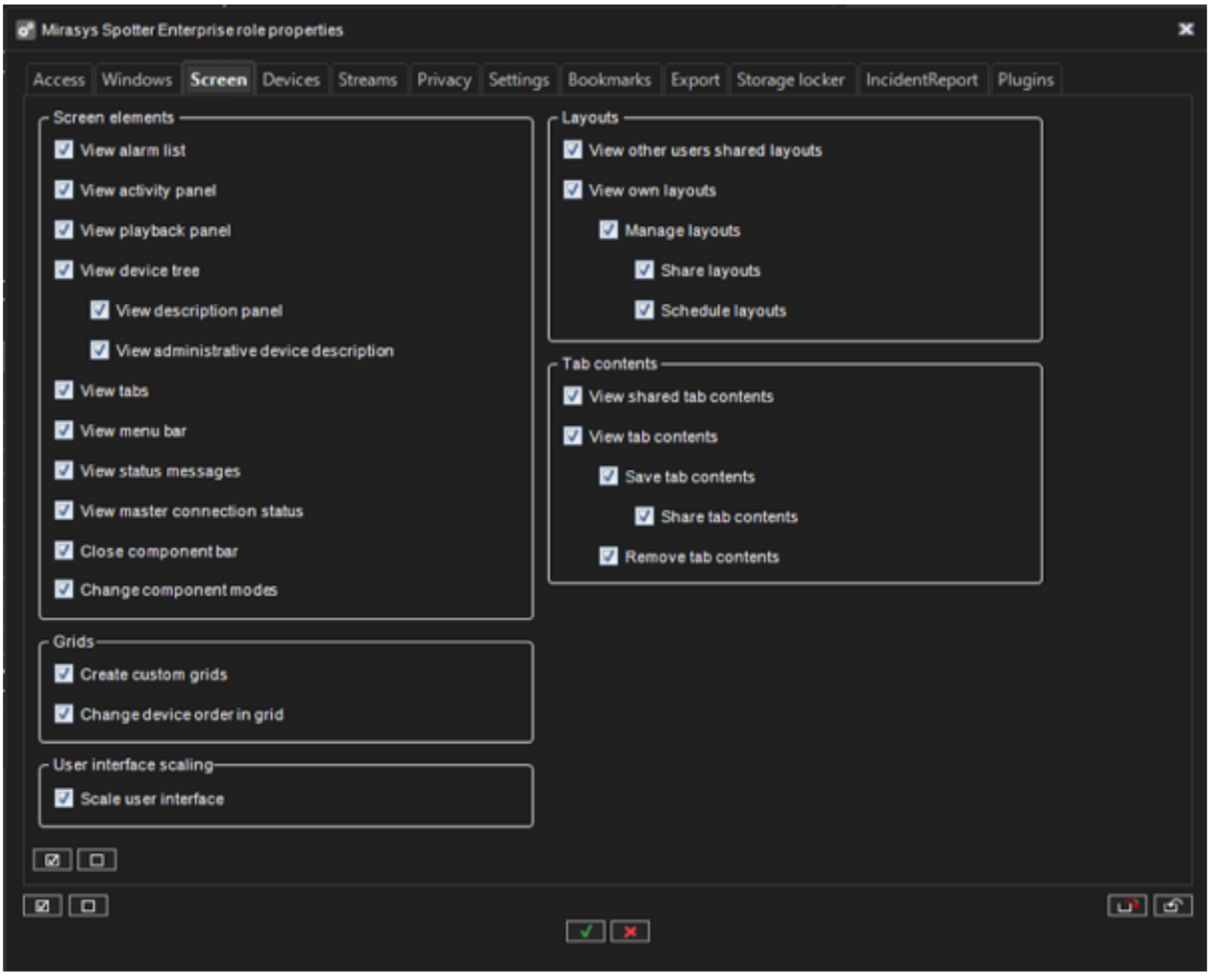
- ☑ Create window
- ☑ Close window
- ☑ Resize window
- ☑ Minimize window
- ☑ Maximize window
- ☑ Restore window
- ☑ Open about window
- □ Limit window count to 6

Tabs

- ☑ Open new device tab
- ☑ Close device tab
- ☑ Rename tab
- ☑ Change tab grid
- □ Limit tab count to 25
- □ Limit tab device count to 40

Screen

The Screen tab contains options for different screen element access and layout access, bookmarks, camera grid and saved camera tabs.



Screen elements

- ☑ View alarm list
- ☑ View activity panel
- ☑ View playback panel
- ☑ View device tree
  - ☑ View description panel
  - ☑ View administrative device description
- ☑ View tabs
- ☑ View menu bar
- ☑ View status messages
- ☑ View master connection status
- ☑ Close component bar
- ☑ Change component modes

Grids

- ☑ Create custom grids
- ☑ Change device order in grid

User interface scaling

- ☑ Scale user interface

Layouts

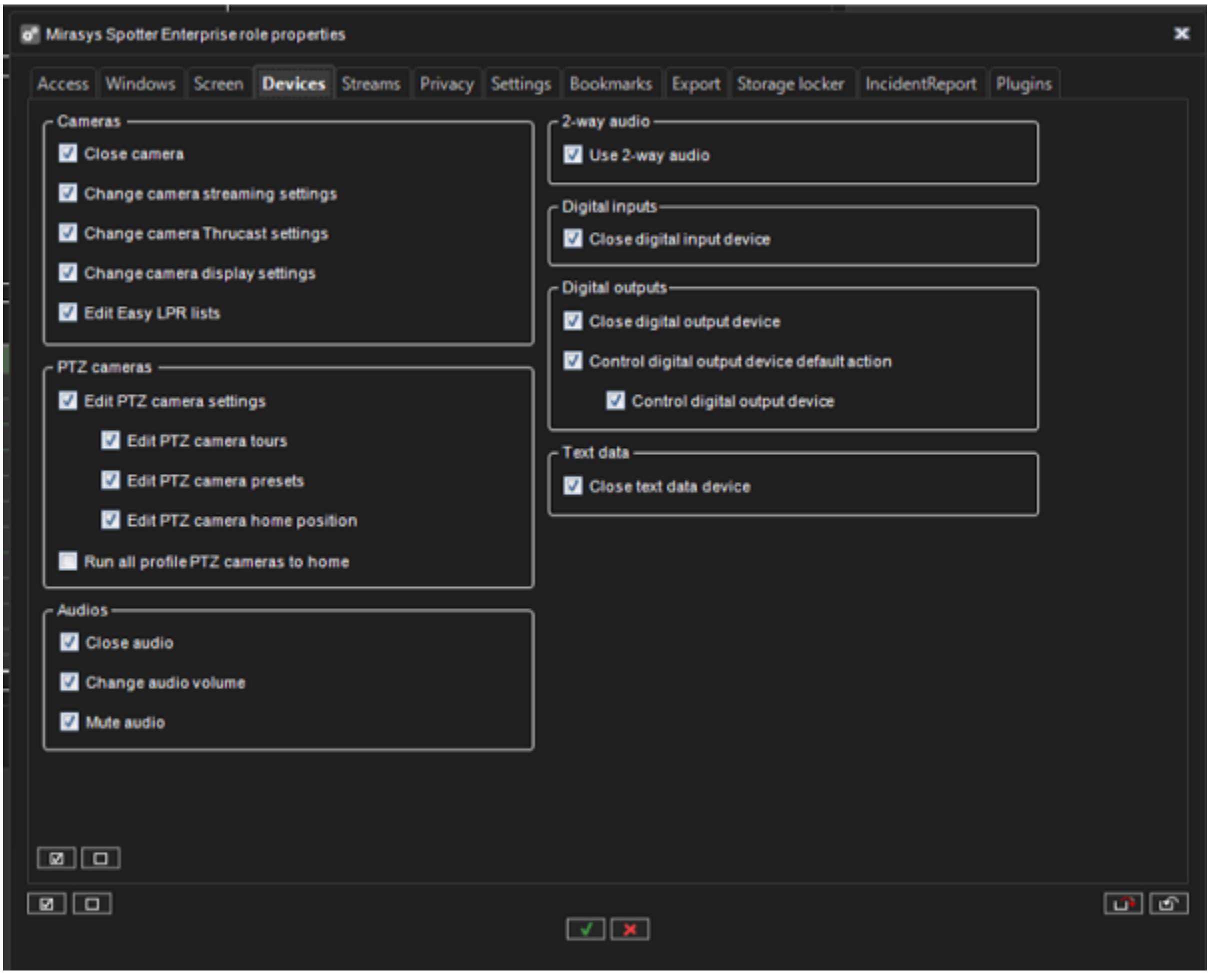
- ☑ View other users shared layouts
- ☑ View own layouts
  - ☑ Manage layouts
    - ☑ Share layouts
    - ☑ Schedule layouts

Tab contents

- ☑ View shared tab contents
- ☑ View tab contents
  - ☑ Save tab contents
    - ☑ Share tab contents
  - ☑ Remove tab contents

Devices

The Devices tab contains options for media control.



Mirasys Spotter Enterprise role properties

Cameras

☑ Close camera

☑ Change camera streaming settings

☑ Change camera Thrucast settings

☑ Change camera display settings

☑ Edit Easy LPR lists

PTZ cameras

☑ Edit PTZ camera settings

☑ Edit PTZ camera tours

☑ Edit PTZ camera presets

☑ Edit PTZ camera home position

□ Run all profile PTZ cameras to home

Audios

☑ Close audio

☑ Change audio volume

☑ Mute audio

2-way audio

☑ Use 2-way audio

Digital inputs

☑ Close digital input device

Digital outputs

☑ Close digital output device

☑ Control digital output device default action

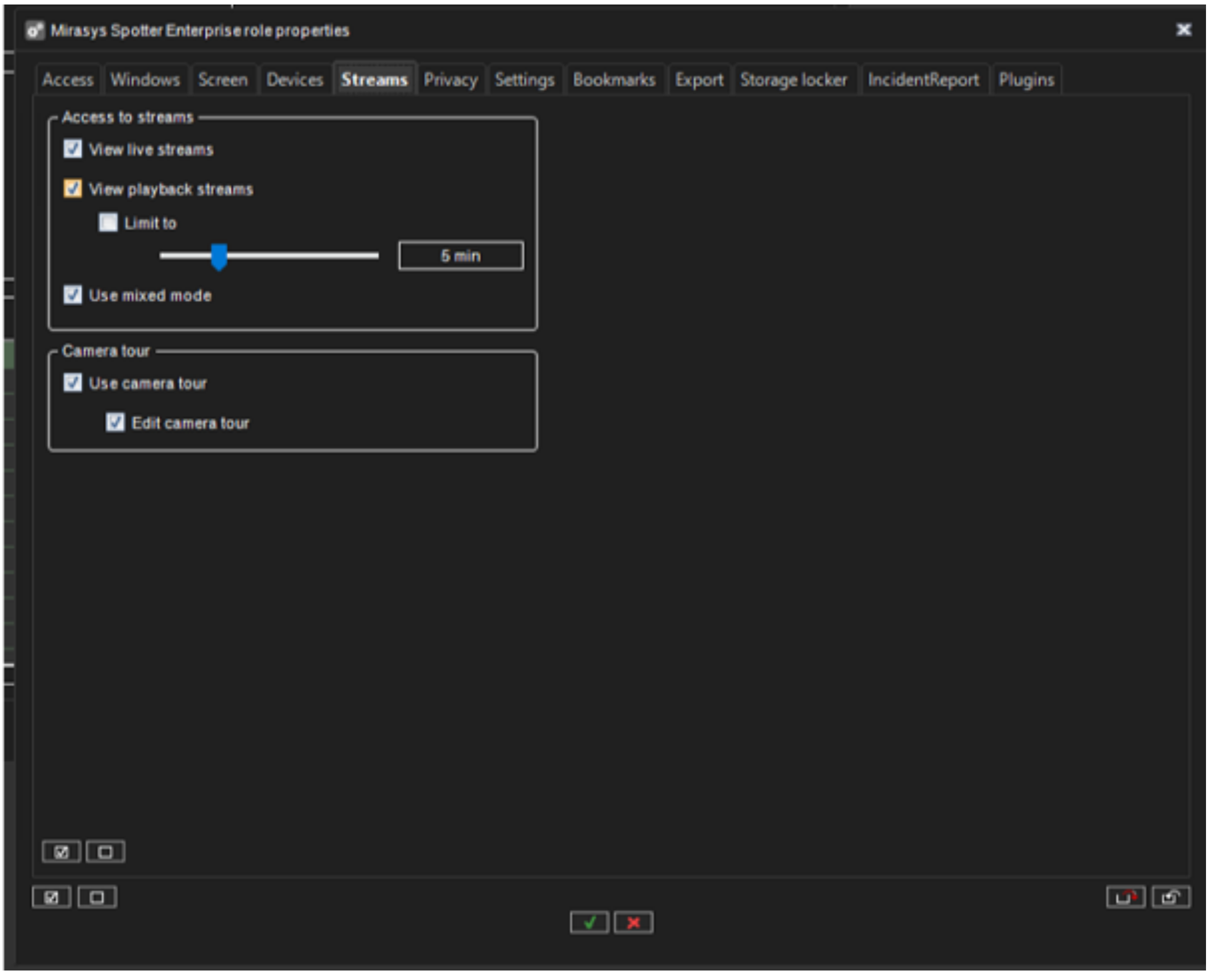
☑ Control digital output device

Text data

☑ Close text data device

Streams

The Streams tab contains options for stream access and exporting.



Mirasys Spotter Enterprise role properties

Access to streams

☑ View live streams

☑ View playback streams

□ Limit to

5 min

☑ Use mixed mode

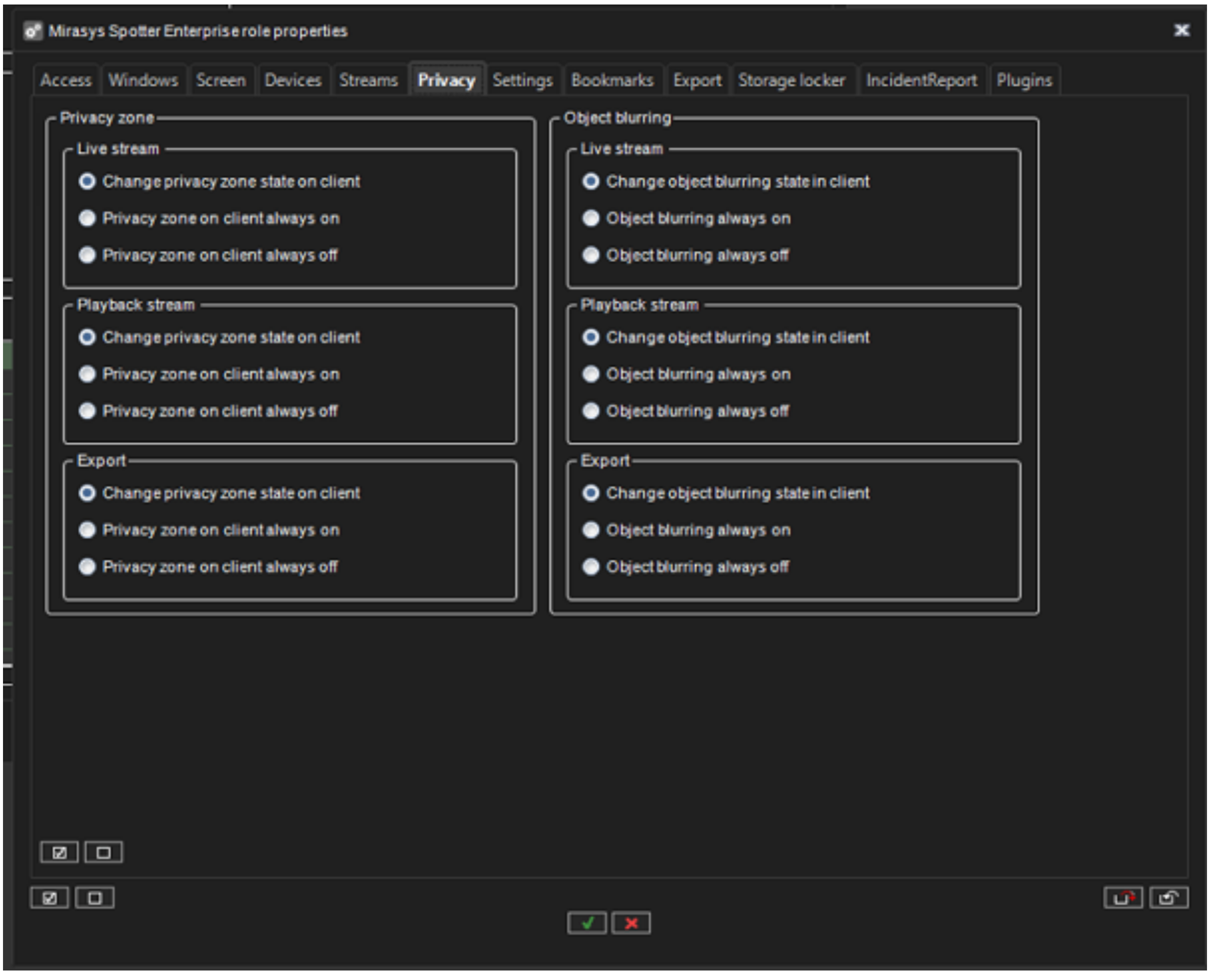
Camera tour

☑ Use camera tour

☑ Edit camera tour

Privacy

The Privacy tab contains options for privacy.



Mirasys Spotter Enterprise role properties

Privacy zone

Live stream

● Change privacy zone state on client
○ Privacy zone on client always on
○ Privacy zone on client always off

Playback stream

● Change privacy zone state on client
○ Privacy zone on client always on
○ Privacy zone on client always off

Export

● Change privacy zone state on client
○ Privacy zone on client always on
○ Privacy zone on client always off

Object blurring

Live stream

● Change object blurring state in client
○ Object blurring always on
○ Object blurring always off

Playback stream

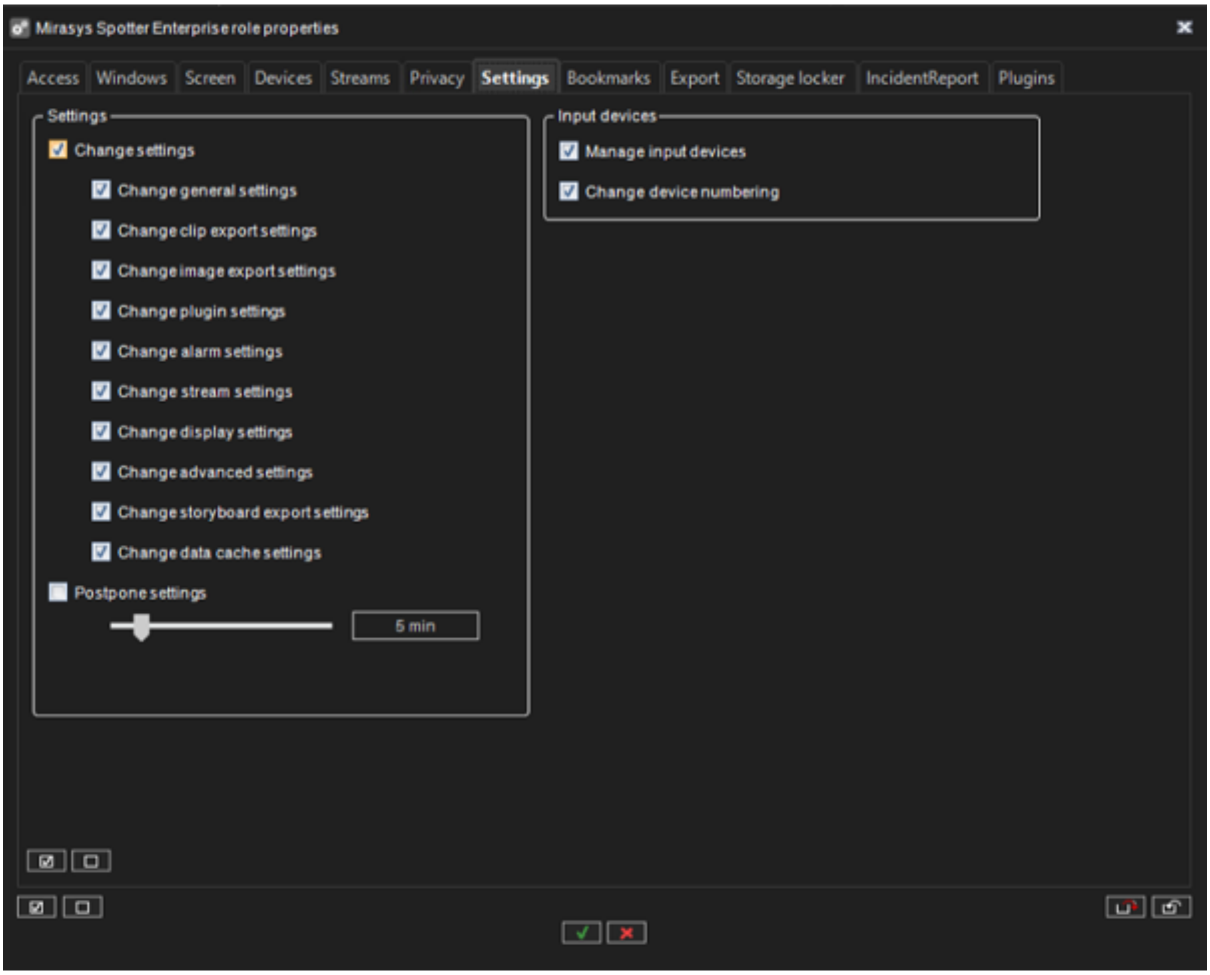
● Change object blurring state in client
○ Object blurring always on
○ Object blurring always off

Export

● Change object blurring state in client
○ Object blurring always on
○ Object blurring always off

Settings

The Settings tab contains options for Spotter settings.



Mirasys Spotter Enterprise role properties

Settings

- ☑ Change settings
  - ☑ Change general settings
  - ☑ Change clip export settings
  - ☑ Change image export settings
  - ☑ Change plugin settings
  - ☑ Change alarm settings
  - ☑ Change stream settings
  - ☑ Change display settings
  - ☑ Change advanced settings
  - ☑ Change storyboard export settings
  - ☑ Change data cache settings
- □ Postpone settings

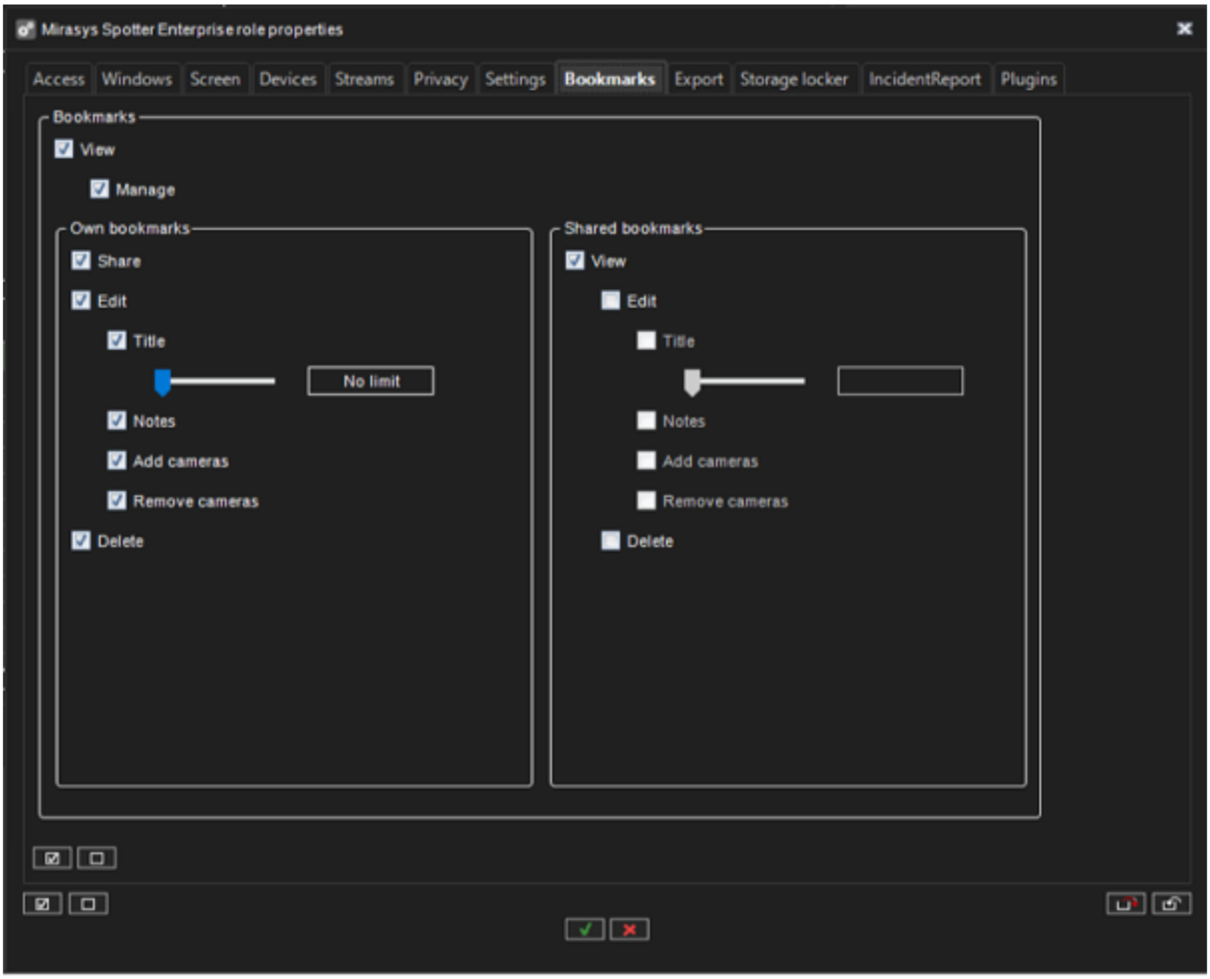
5 min

Input devices

- ☑ Manage input devices
- ☑ Change device numbering

Bookmarks

The Bookmarks tab contains options for bookmarks



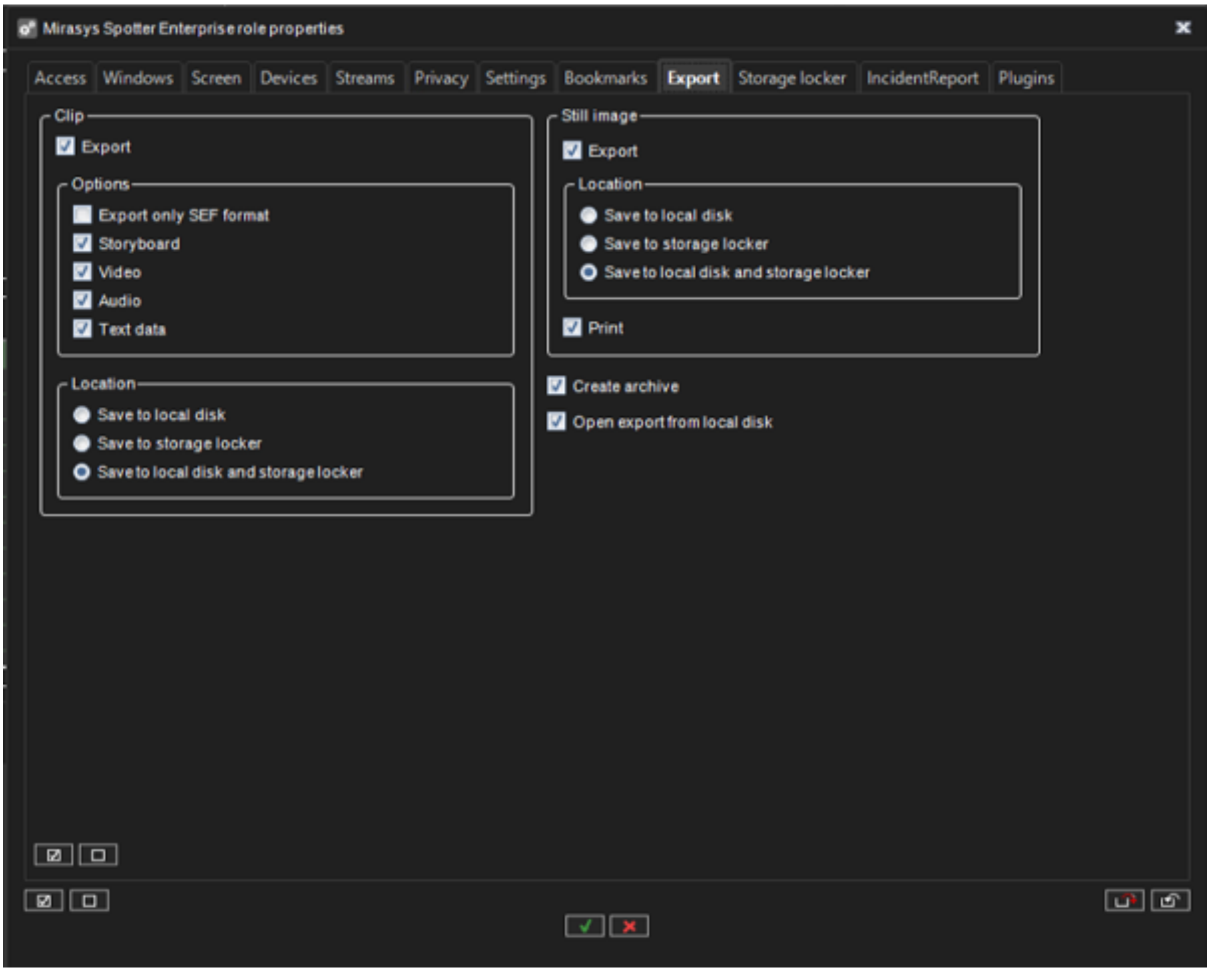
Bookmarks
- ☑ View
  - ☑ Manage

Own bookmarks
- ☑ Share
- ☑ Edit
  - ☑ Title
    - No limit
  - ☑ Notes
  - ☑ Add cameras
  - ☑ Remove cameras
- ☑ Delete

Shared bookmarks
- ☑ View
- □ Edit
  - □ Title
  - □ Notes
  - □ Add cameras
  - □ Remove cameras
- □ Delete

Export

The Export tab contains options for Export functions



Mirasys Spotter Enterprise role properties

Clip

☑ Export

Options

- □ Export only SEF format
- ☑ Storyboard
- ☑ Video
- ☑ Audio
- ☑ Text data

Location

- ○ Save to local disk
- ○ Save to storage locker
- ● Save to local disk and storage locker

Still image

☑ Export

Location

- ○ Save to local disk
- ○ Save to storage locker
- ● Save to local disk and storage locker

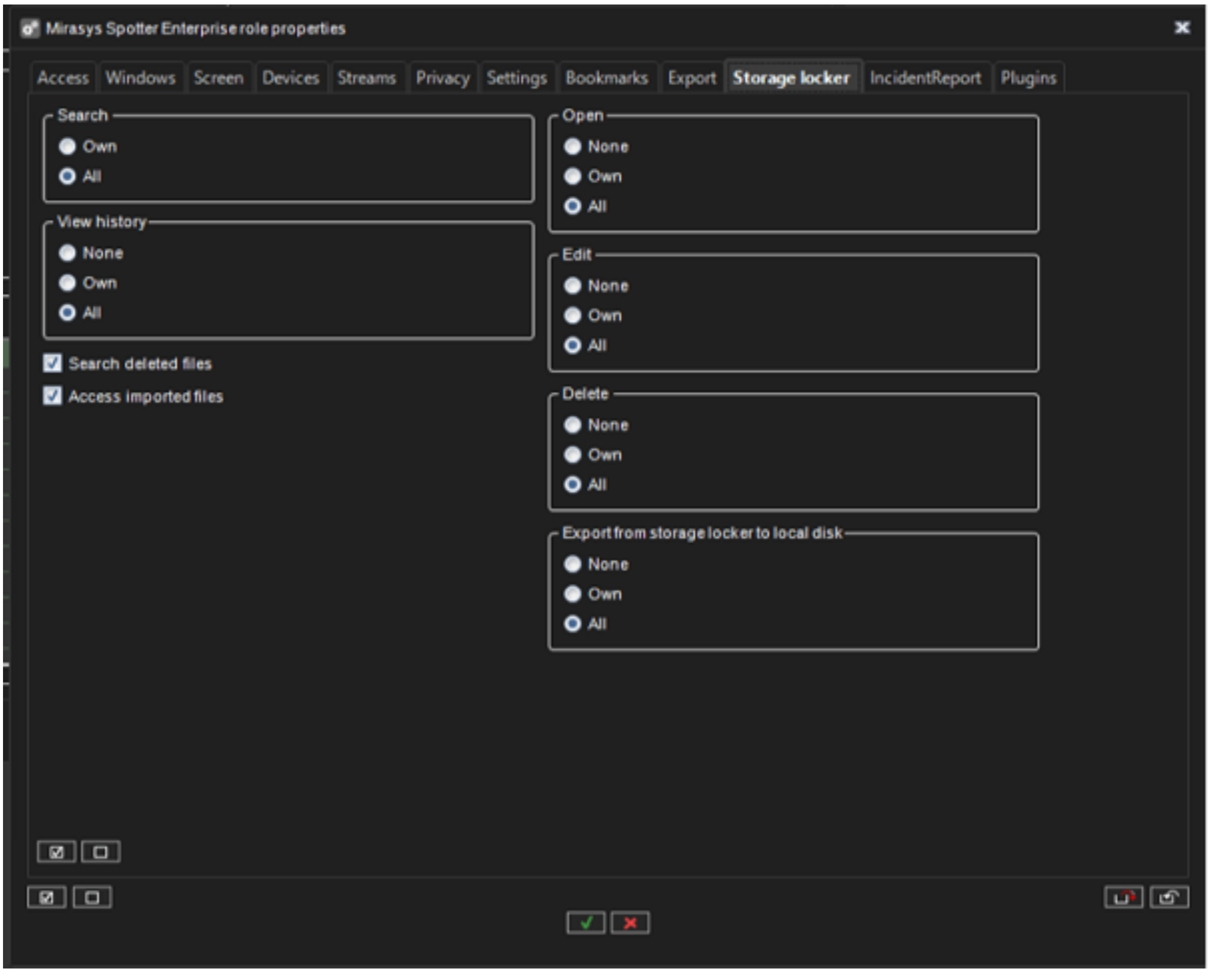
☑ Print

☑ Create archive

☑ Open export from local disk

Storage Locker

The Storage Locker tab contains options for the Storage Locker plugin.



Search
○ Own
◉ All

View history
○ None
○ Own
◉ All

☑ Search deleted files
☑ Access imported files

Open
○ None
○ Own
◉ All

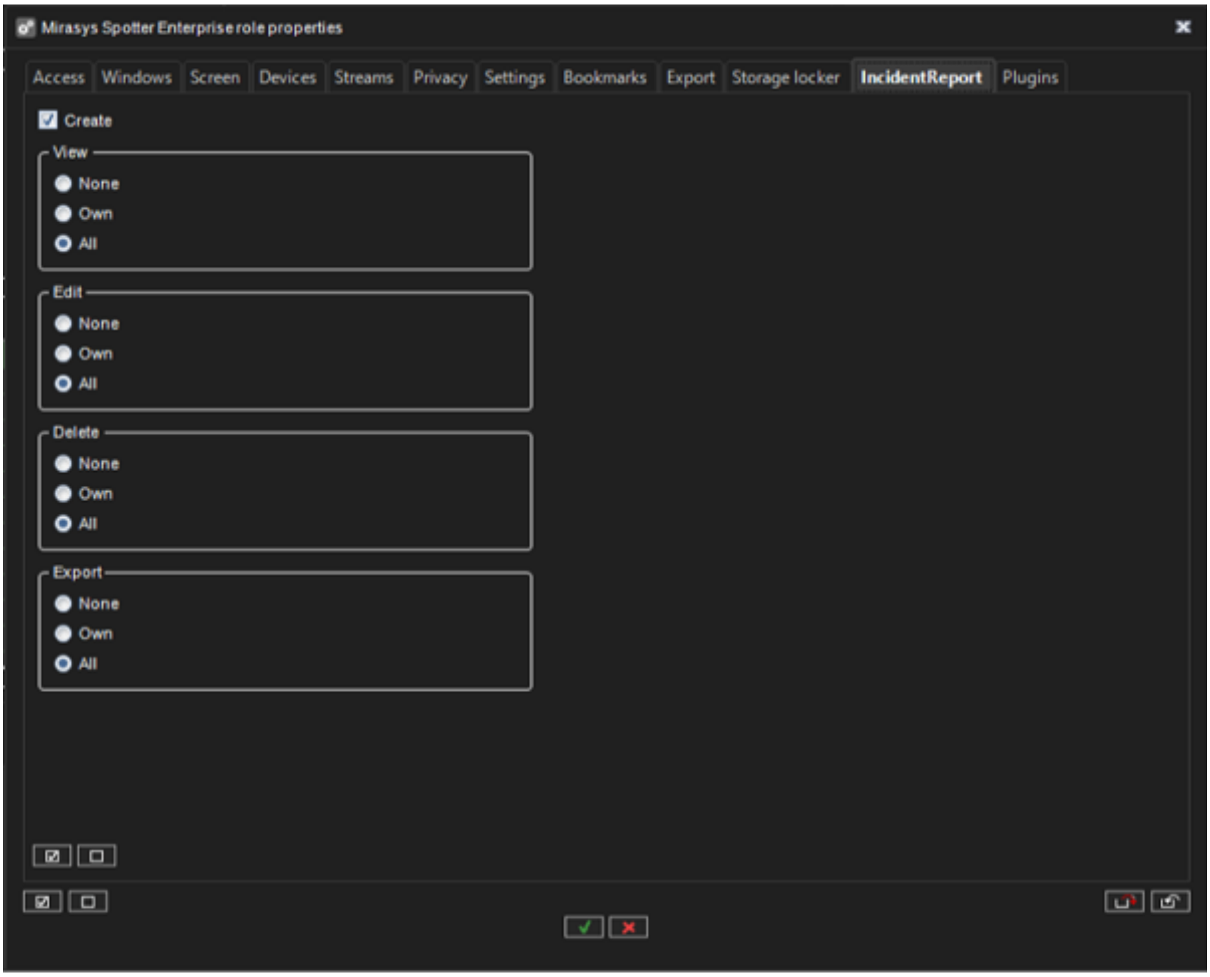
Edit
○ None
○ Own
◉ All

Delete
○ None
○ Own
◉ All

Export from storage locker to local disk
○ None
○ Own
◉ All

Incident Reporting

The Incident Reporting tab contains options for the Incident Reporting plugin



☑ Create

View
○ None
○ Own
● All

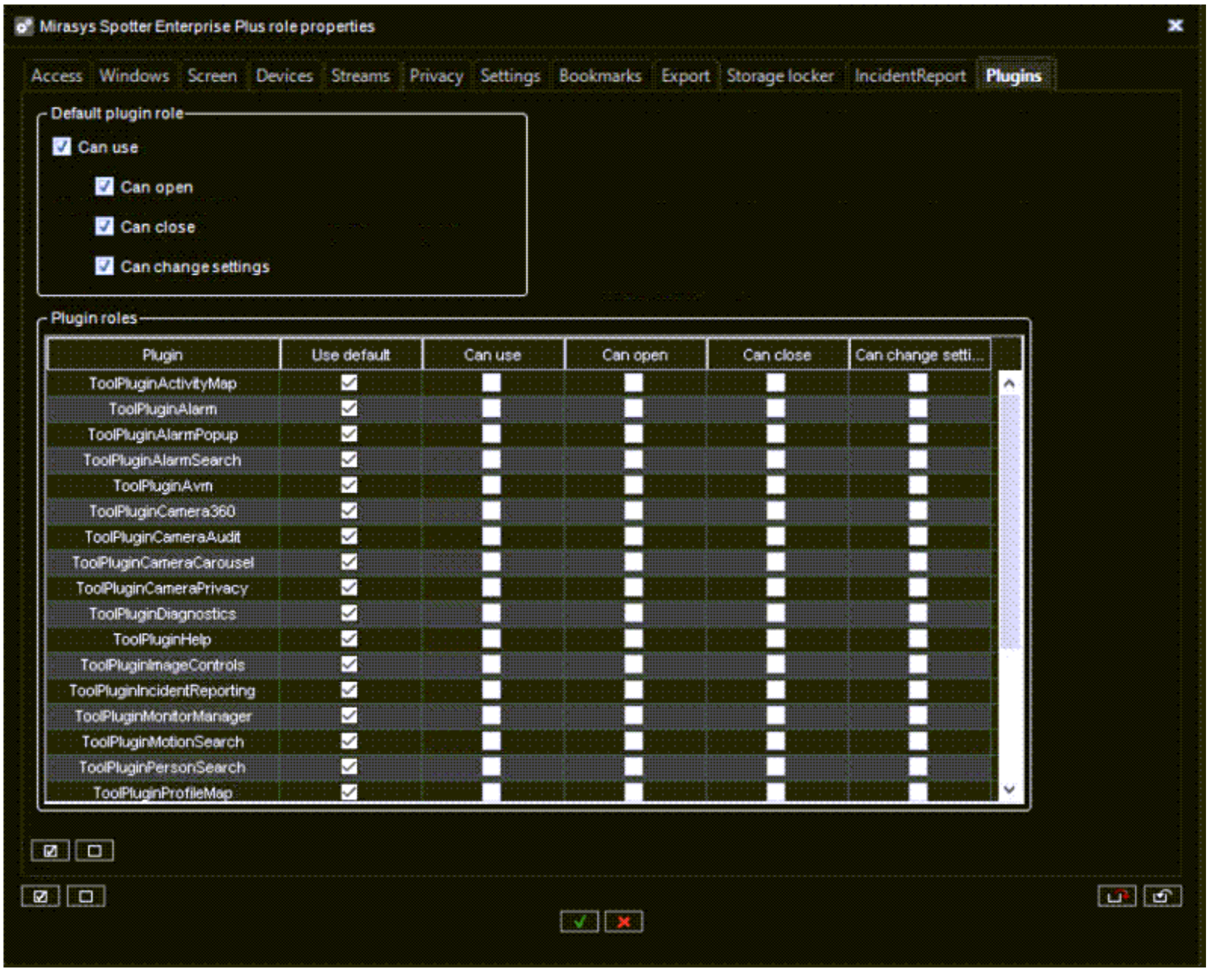
Edit
○ None
○ Own
● All

Delete
○ None
○ Own
● All

Export
○ None
○ Own
● All

Plugins

The Plugins tab contains options for Spotter plugins.



Mirasys Spotter Enterprise Plus role properties

Access | Windows | Screen | Devices | Streams | Privacy | Settings | Bookmarks | Export | Storage locker | IncidentReport | **Plugins**

Default plugin role

☑ Can use

- ☑ Can open
- ☑ Can close
- ☑ Can change settings

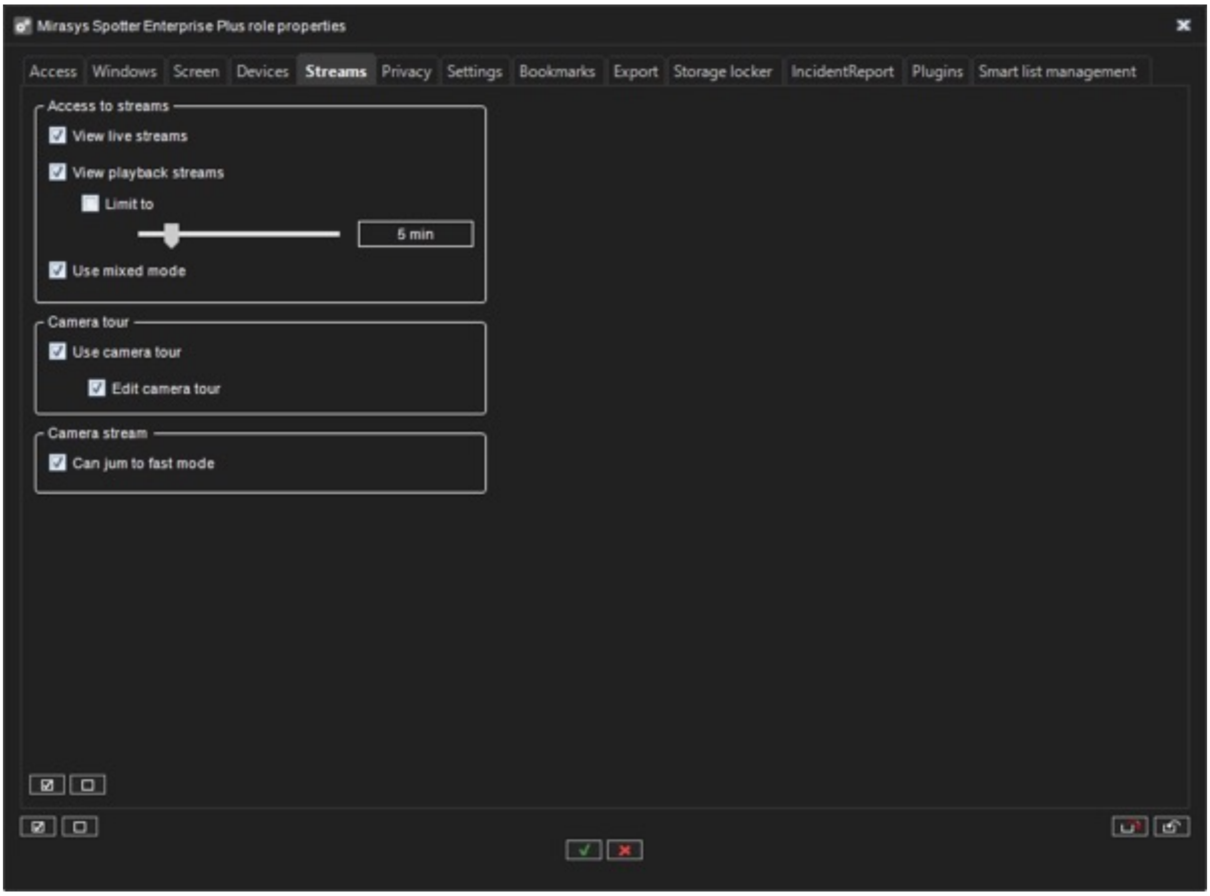
Plugin roles

Plugin	Use default	Can use	Can open	Can close	Can change setti...
ToolPluginActivityMap	☑	□	□	□	□
ToolPluginAlarm	☑	□	□	□	□
ToolPluginAlarmPopup	☑	□	□	□	□
ToolPluginAlarmSearch	☑	□	□	□	□
ToolPluginAvm	☑	□	□	□	□
ToolPluginCamera360	☑	□	□	□	□
ToolPluginCameraAudit	☑	□	□	□	□
ToolPluginCameraCarousel	☑	□	□	□	□
ToolPluginCameraPrivacy	☑	□	□	□	□
ToolPluginDiagnostics	☑	□	□	□	□
ToolPluginHelp	☑	□	□	□	□
ToolPluginImageControls	☑	□	□	□	□
ToolPluginIncidentReporting	☑	□	□	□	□
ToolPluginMonitorManager	☑	□	□	□	□
ToolPluginMotionSearch	☑	□	□	□	□
ToolPluginPersonSearch	☑	□	□	□	□
ToolPluginProfileMap	☑	□	□	□	□

Each plugin behaviour can be either default or custom. The default behaviour can be controlled from the ”Default plugin role” controls.

Playback Speed Role

Spotter playback automatic speed adjustment can be enabled or disabled in the Spotter role settings “Streams” tab.



Access to streams

☑ View live streams

☑ View playback streams

☐ Limit to

5 min

☑ Use mixed mode

Camera tour

☑ Use camera tour

☑ Edit camera tour

Camera stream

☑ Can jum to fast mode

In the Camera streams group, there is a selection for fast playback mode. If selected, with 2x, 4x, and 8x playback speeds, if the playback cannot keep the pace because of too much load, it will jump to fast forward/backward. By default, automatic playback speed adjustment is not selected.

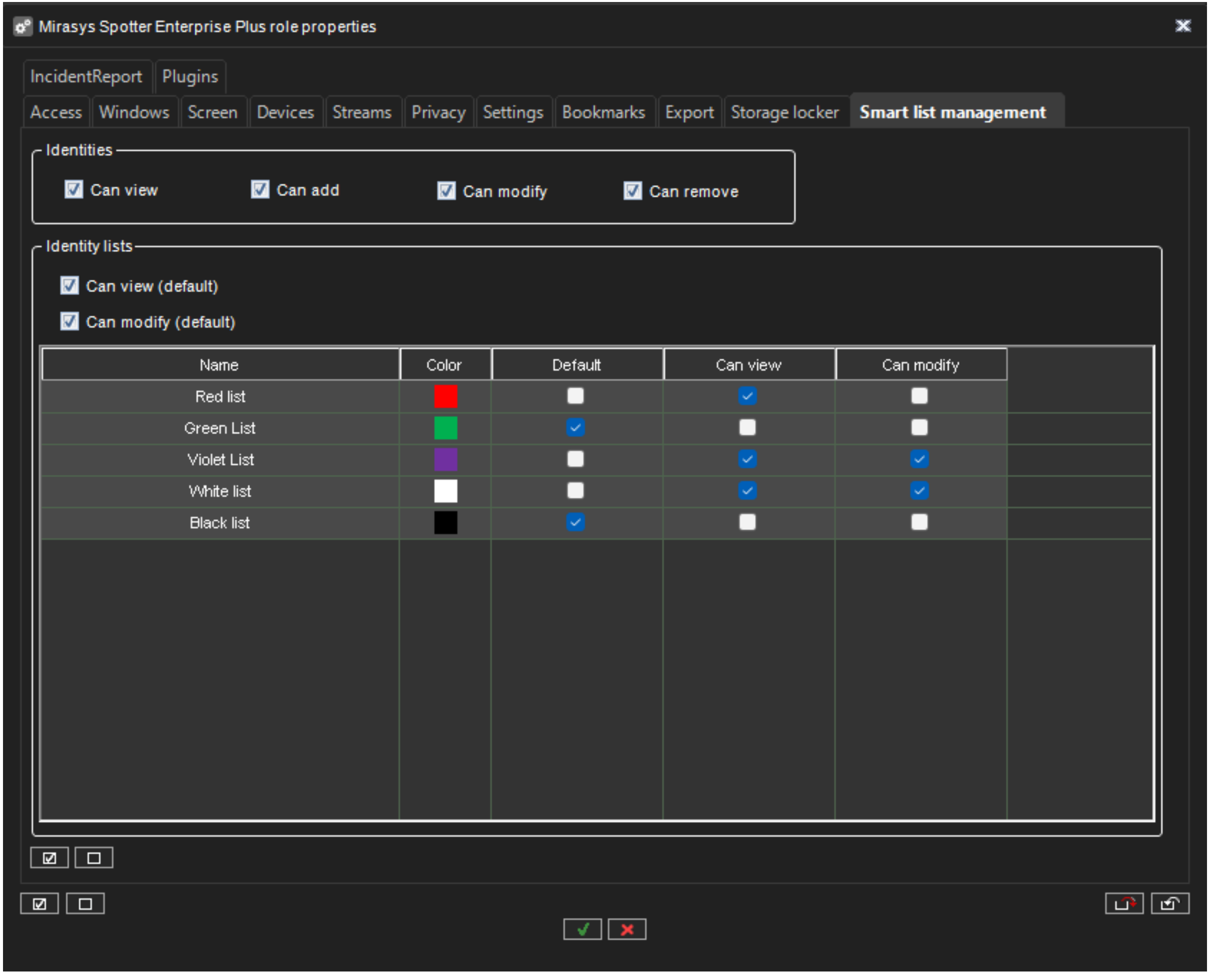
Smart List Management role

The Spotter List Management plugin can be enabled on the Spotter user role settings, where it is also possible to limit the permissions to manage identities and identity lists.

Smart list management properties

The “Smart list management“ tab contains role properties related to smart list management functionality:

- Possibility to view, add, modify, and remove identities.
- Possibility to view and modify identity lists (default properties and properties for each list separately).



Mirasys Spotter Enterprise Plus role properties

IncidentReport | Plugins
Access | Windows | Screen | Devices | Streams | Privacy | Settings | Bookmarks | Export | Storage locker | Smart list management

Identities

☑ Can view ☑ Can add ☑ Can modify ☑ Can remove

Identity lists

☑ Can view (default)

☑ Can modify (default)

Name	Color	Default	Can view	Can modify
Red list	🟥	□	☑	□
Green List	🟩	☑	□	□
Violet List	🟪	□	☑	☑
White list	⬜	□	☑	☑
Black list	⬛	☑	□	□

Figure 13 “Smart list management“ tab

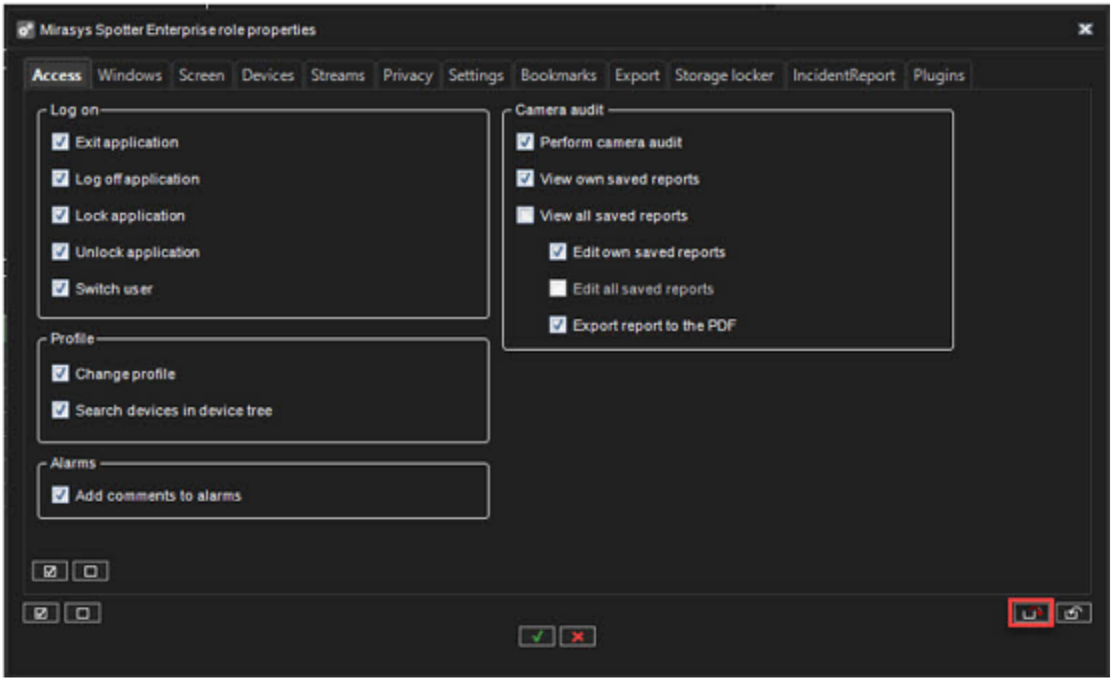
Spotter Web role

Spotter Web role enables new Spotter Web and Spotter Mobile usage

Exporting and Importing User Role Settings

Exporting User role settings

- Click **Export user role settings to file**



Mirasys Spotter Enterprise role properties

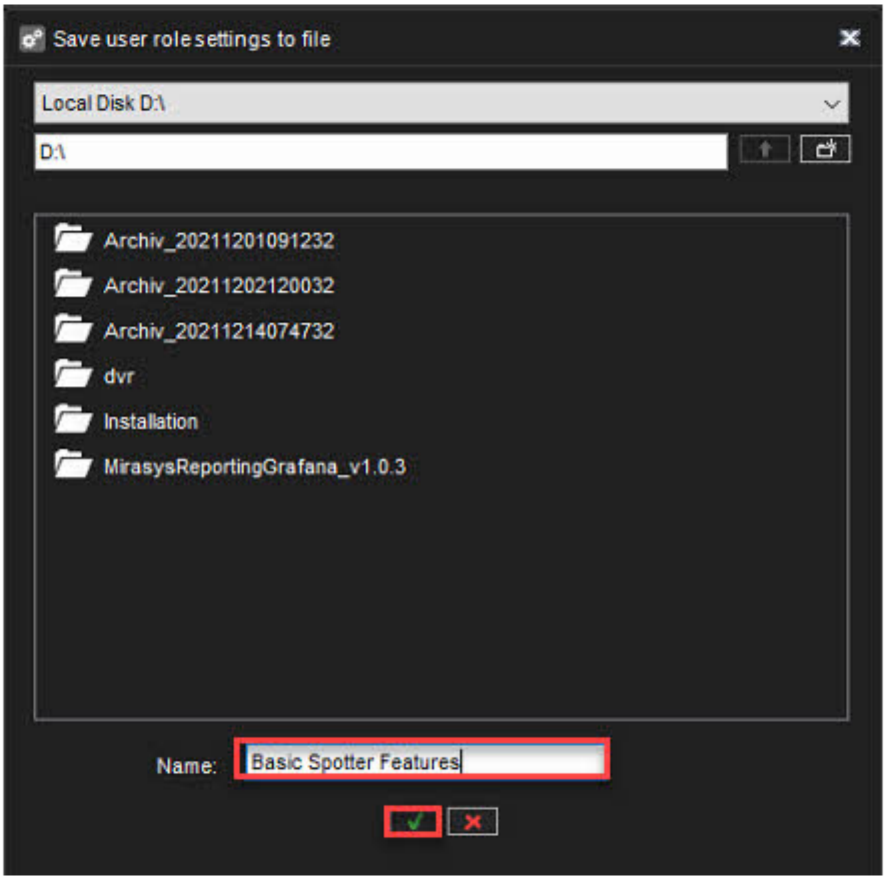
Log on
☑ Exit application
☑ Log off application
☑ Lock application
☑ Unlock application
☑ Switch user

Profile
☑ Change profile
☑ Search devices in device tree

Alarms
☑ Add comments to alarms

Camera audit
☑ Perform camera audit
☑ View own saved reports
☐ View all saved reports
☑ Edit own saved reports
☐ Edit all saved reports
☑ Export report to the PDF

- Select destination
- Set the name of the file
- Click **OK**



Save user role settings to file

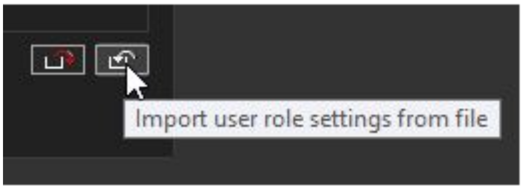
Local Disk D:\

D:\

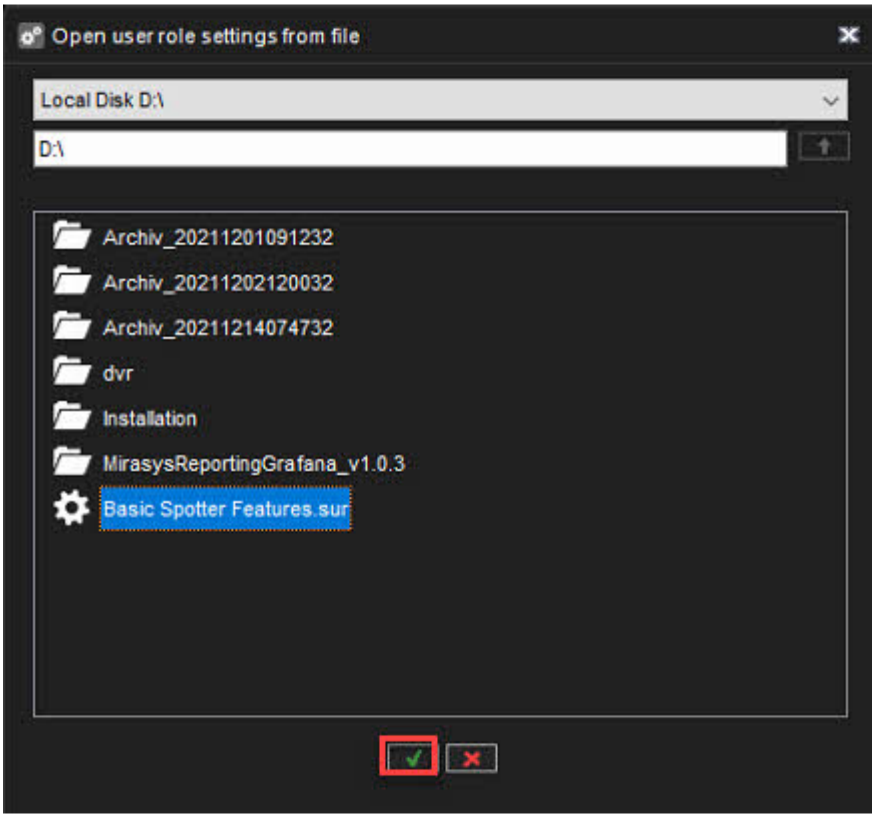
Name: Basic Spotter Features

Importing User role settings

- Click **Import user role settings from the file**



- Select file(.sur)
- Click **OK**



Two-factor authentication

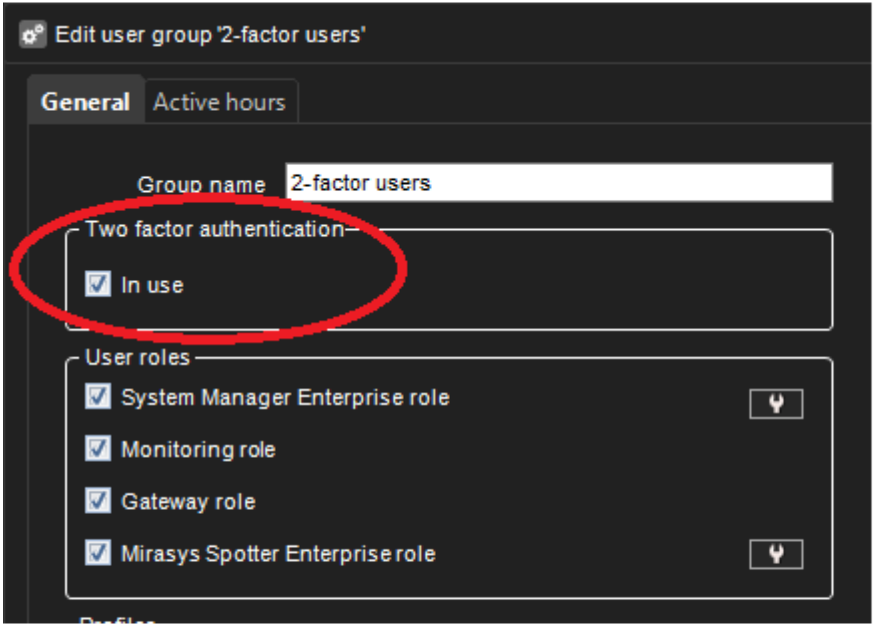
Two-factor authentication is functionality to improve the user's identification by requiring the username and password and a code from an external physical device.

This makes it practically impossible, e.g. certain user groups (e.g. system administrators), to use shared credentials.

(Using shared credentials would make it almost impossible, e.g. to monitor specific user actions from the audit logs later on.)

Setup:

- The admin enables the 2-factor authentication for the specific user group.



Edit user group '2-factor users'

Group name: 2-factor users

Two factor authentication

☑ In use

User roles

☑ System Manager Enterprise role

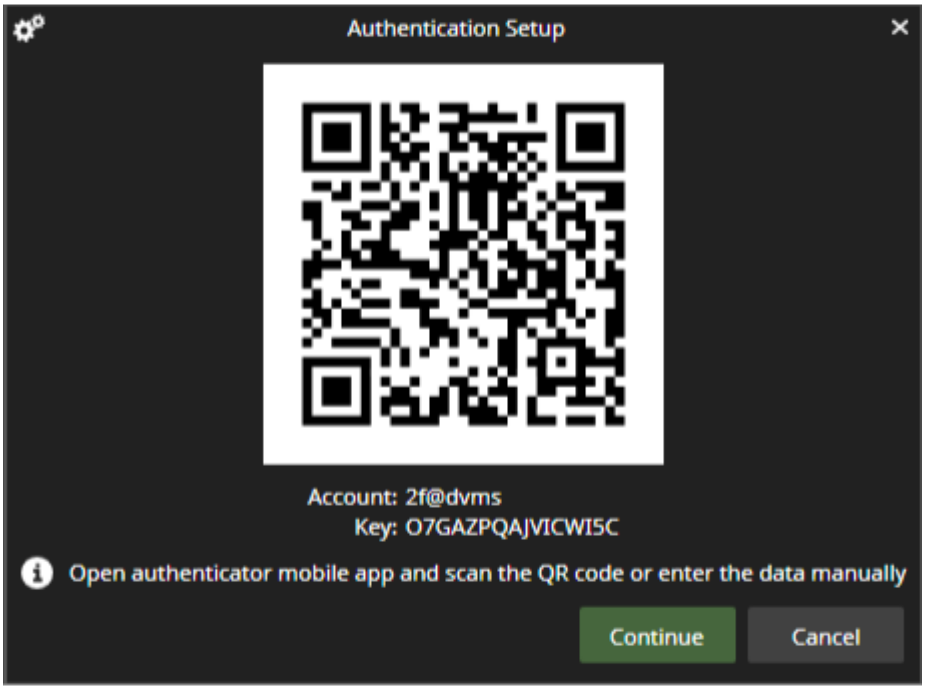
☑ Monitoring role

☑ Gateway role

☑ Mirasys Spotter Enterprise role

- When the user in the group tries to log in for the first time, the user is requested to use or install the 2-factor authentication client (e.g. Authy, Google authenticator, MS Authenticator (available for free)) on his/her mobile device.
- The VMS and the authentication client are then synchronized with the software with VMS.
- This happens by transferring the "secret key" generated by the VMS to the authentication software via QR code or directly typing it to the software.

Example below:



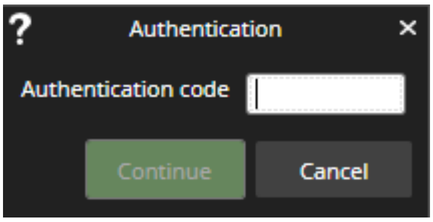
Account: 2f@dvms
Key: O7GAZPQAJVICWI5C

Open authenticator mobile app and scan the QR code or enter the data manually

- After that, the authentication client automatically generates new one-time passwords.
  a. (The passwords change periodically and are kept in sync as the VMS clocks and the authentication app have the same time.
  b. Note that this does not require any direct data communication link between the software.)

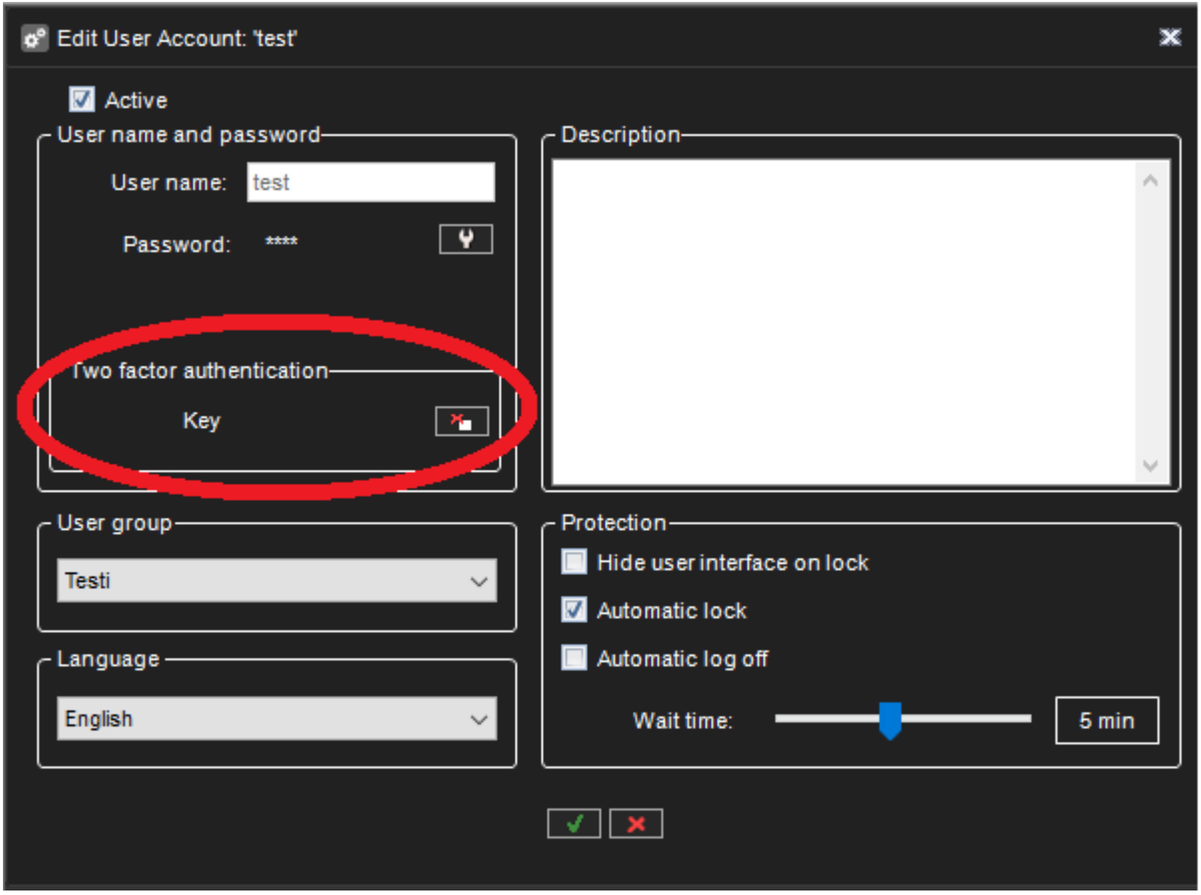
Login:

1. The user provides the standard credentials to VMS (username, password)
2. The VMS requests an authentication code from the authentication app for each login.
3. The user provides the one-time password from the authentication app. The user types them to the VMS client.



Maintenance:

1. If the user forgets his / her 2-factor secret key, the administrator can then reset the key from the system manager.
2. After the 2-factor secret key reset, the user needs to update the private key next time he/she logs in. (See step 2).



Edit User Account: 'test'

☑ Active

User name and password

User name: test

Password: ****

Two factor authentication

Key

Description

User group

Testi

Language

English

Protection

□ Hide user interface on lock

☑ Automatic lock

□ Automatic log off

Wait time: 5 min

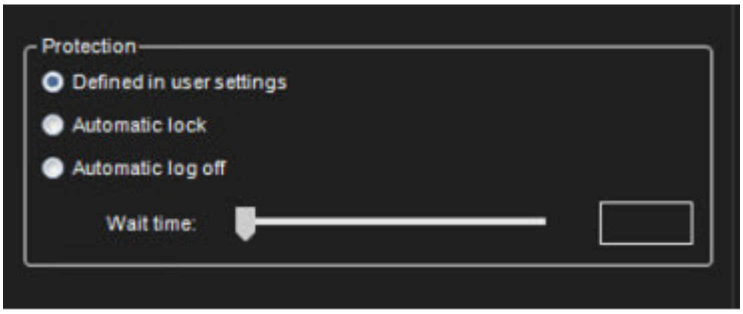
Protection

Protection group box is added in user group / general settings.

As default, "**Defined in user settings**" is set and Automatic lock, Automatic log off are not selected and Wait time settings is disabled.

Only one of the check box selections can be set at the time.

If user group level automatic lock / log off settings are selected, then user level automatic lock / log off settings are not enabled in user account settings



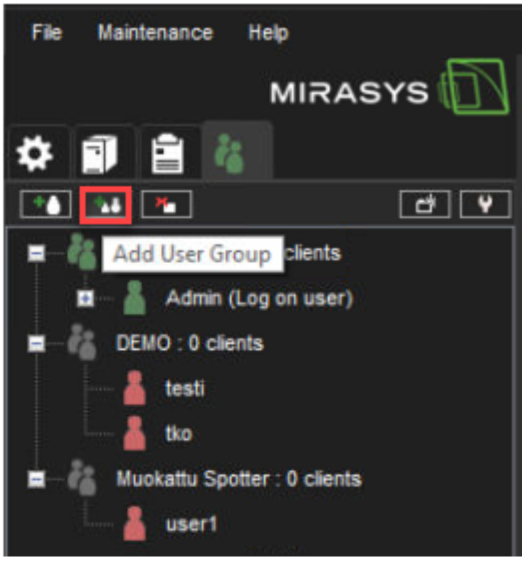
Protection
● Defined in user settings
○ Automatic lock
○ Automatic log off
Wait time:

Automatic lock and Automatic log off values

- 1-5 min, 10, 15, 20, 30 min, 1-12 hour and 24 hour

Creating a customer-specific User Group

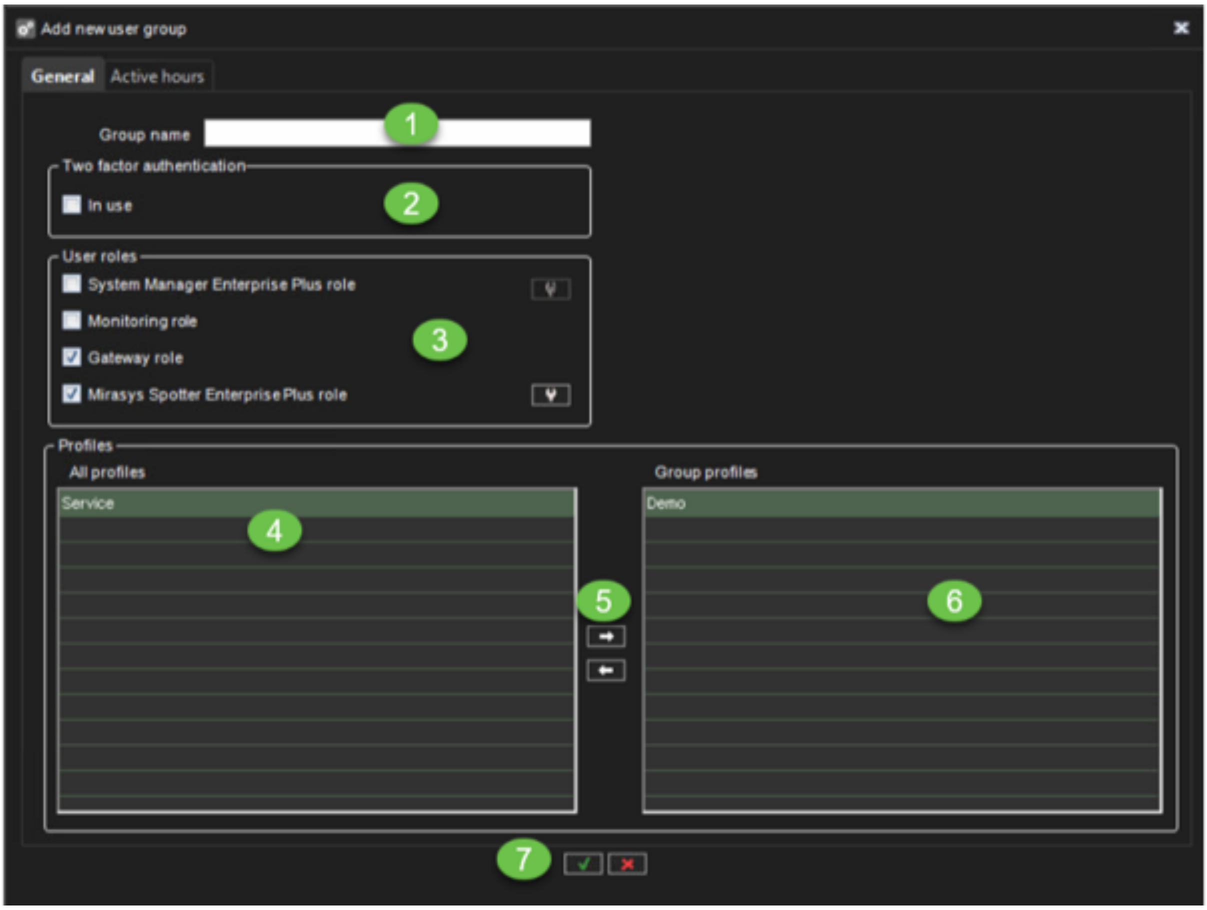
1. Click **Add User Group**



2. Type a name for the group in the **Group name** box
3. Enable **Two-factor authentication**, if needed
4. Select the **User roles** for the group.

5. Select the **Profile** or **Profiles** you want to assign to the user group.
6. Click the right arrow button or drag the profiles from the left panel to the group profiles box
7. Check that correct profiles is found
8. Click **Ok** to confirm user group creation

Tip: *To select more than one profile at a time, keep the SHIFT, or CTRL key pressed.*



Add new user group

General | Active hours

Group name

Two factor authentication

☐ In use

User roles

☐ System Manager Enterprise Plus role

☐ Monitoring role

☑ Gateway role

☑ Mirasys Spotter Enterprise Plus role

Profiles

All profiles: Service

Group profiles: Demo

Editing a User group

To edit a user group (whether system or domain-**based):**

1. Open the **Users** tab.
2. Click on the user group you want to edit.
3. You can edit the following settings:
    a. Type a name for the group in the **Group name** box.
    b. Select the user roles for the group.

   c. Select the profile or profiles you want to assign to the user group. Click the right arrow button or drag the profiles from the left pane to the right.

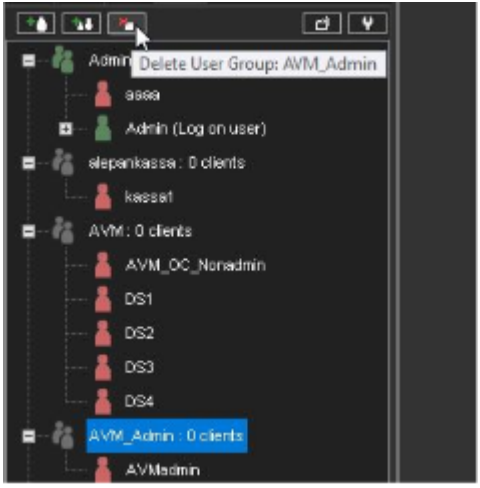
4. Click **OK** to save the changes.

- **Tip:** *To select more than one profile at a time, keep the SHIFT, or CTRL key pressed.*

Deleting a user group

To delete a user group (whether system or domain-**based):**

- Open the **Users** tab.
- Click on the user group you want to delete. Note that you cannot delete the default **Administrators** group.



3. Click **Delete User Group** in the upper-left corner.

4. Click **OK** to delete the group.

Note: *Domain-based (LDAP) user groups cannot be deleted through System Manager. If deleted, an LDAP group is removed from System Manager, but the domain group is not affected.*

Domain Based User Groups (LDAP)

The system supports domain-level user rights integration (Microsoft Active Directory, LDAP), enabling users to be synchronized from domain groups.

Domain-based users can log into the VMS system with their domain usernames and passwords.

By default, user group rights are synchronized with their parent domain every 30 minutes.

Please contact your system supplier if f you need to change the default interval.

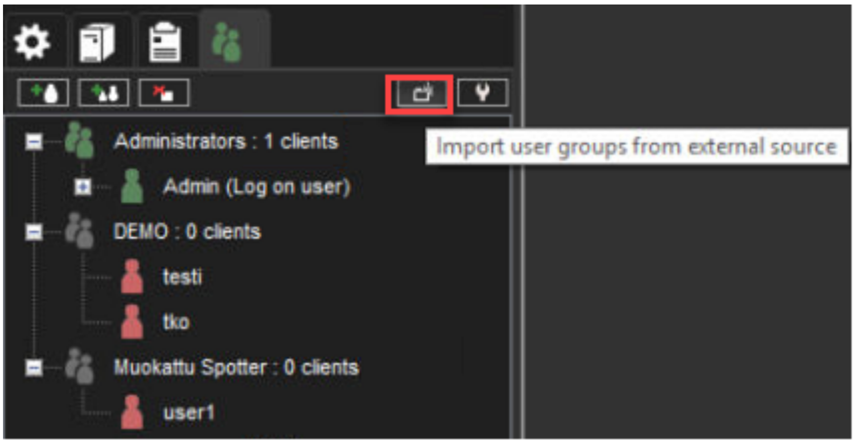
This feature requires a license update.

To add a new domain-based user group to the system:

- Click **Import User Groups from an external source** in the upper-left corner of the **Users** tab

The Master Server needs to be connected to a domain for the button to be displayed.

If the server is not connected to a domain, the button is not visible.


Import user groups from external source
Administrators : 1 clients
Admin (Log on user)
DEMO : 0 clients
testi
tko
Muokattu Spotter : 0 clients
user1

2. Type the name of the domain into the **Domain name** dialogue box.

3. Select whether to get all user groups or to search for specific groups.

If you want to search specific groups by name, you can add a search criterion based on the text string being equal to the group name, contained in the group name, or the group name starting or ending in the text string.

4. Select whether to skip or include open user groups.

5. Select whether to clear or keep previous search results.

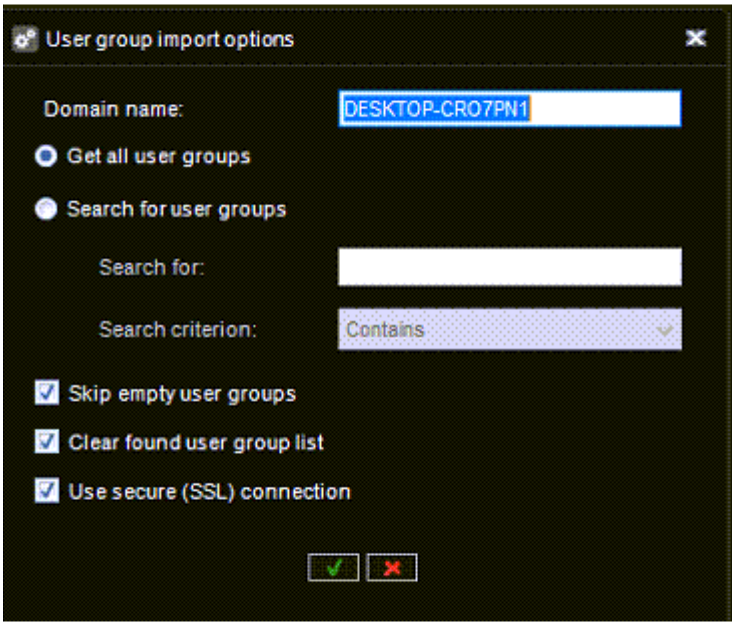
6. Enable **Use secure(SSL) connection**. If needed

7. Click **Ok**.

8. In the **Import user groups** window, select the user groups you wish to import from the domain.

9. Click **Ok** to import the selected groups.

10. Edit the imported user groups to set their user roles as instructed below.



User group import options

Domain name: DESKTOP-CRO7PN1

● Get all user groups

○ Search for user groups

Search for:

Search criterion: Contains

☑ Skip empty user groups

☑ Clear found user group list

☑ Use secure (SSL) connection

Creating a customer-specific user

To add a new user to the system:

- Open the **Users** tab.
- Click the name of the user group to which you want to add the user.
  - Note that you can only add users to the system's native groups, not in domain-based groups.
- Click **Add User** in the upper-left corner of the Users tab. The Add User dialogue box is shown.

- Do the following:
    - Type a name for the account in the **Username** box.
    - To add a password to the account, click **Change password** and type the password two times.
    - Type an optional description about the user account.
    - Use the pull-down menu to select the user group into which you want to assign to the user.
    - Select the user interface language for the user.
    - Set protection settings for the programs:
        - **Hide user interface on lock**
        - **Automatic lock**
        - **Automatic log-off**
        - **Wait time**: if the user does not use the program for the specified time, the program is locked, or the user is logged off.

Note: Users can change their passwords and user interface language in the Spotter program.

User account settings

User account settings contain the following options:

- Account status
- Password
- Two-factor authentication key management, see more from Two-factor authentication
- User group
- Language
- Protection settings
    - Hide user interface on lock
    - Automatic lock
    - Automatic log off

Supported languages

- Arabic
- Chinese
- Czech
- Danish
- Dutch
- Estonian
- Finnish
- French
- German
- Hungarian

- Icelandic
- Italian
- Norwegian
- Polish
- Portuguese
- Russian
- Slovenian
- Spanish
- Swedish
- Thai

Disabling or Activating a User Account

If you want to prevent a user from logging on to the system but want to keep the user account for later use, you can disable the account.

You can activate the account when the user is again permitted to log in to the system.

To disable or activate a user account:

- On the **Users** tab, select the user account
- Click **Edit User Account**
- Do one of the following:
- To disable the account, clear the check box **Active**.
- To activate the account, select the check box **Active**.

4. Click **OK**.

Note: *Domain-based (LDAP) users cannot be deleted or removed with System Manager.*

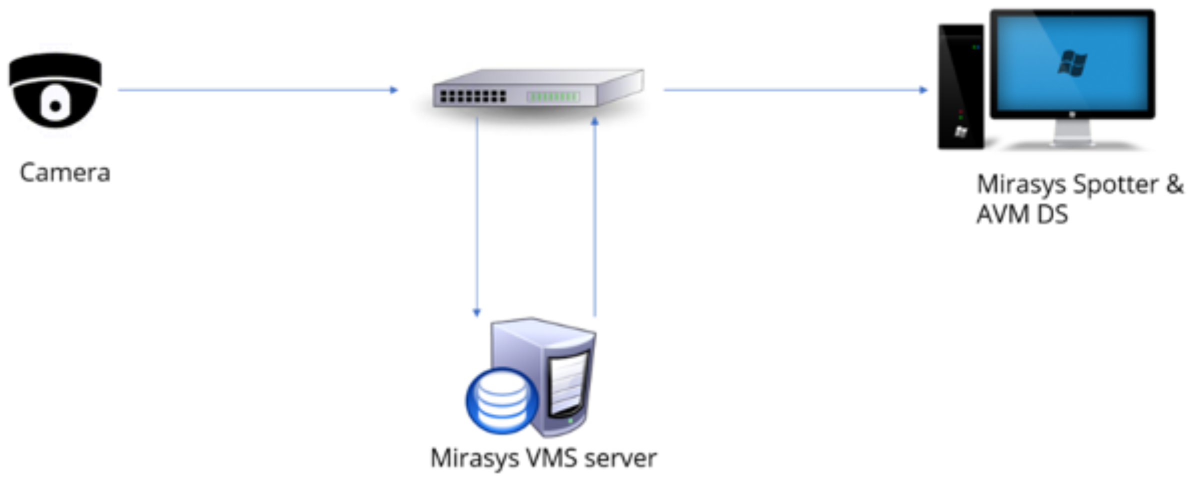
TruCast

TruCast is the direct camera video streaming feature in Mirasys VMS.

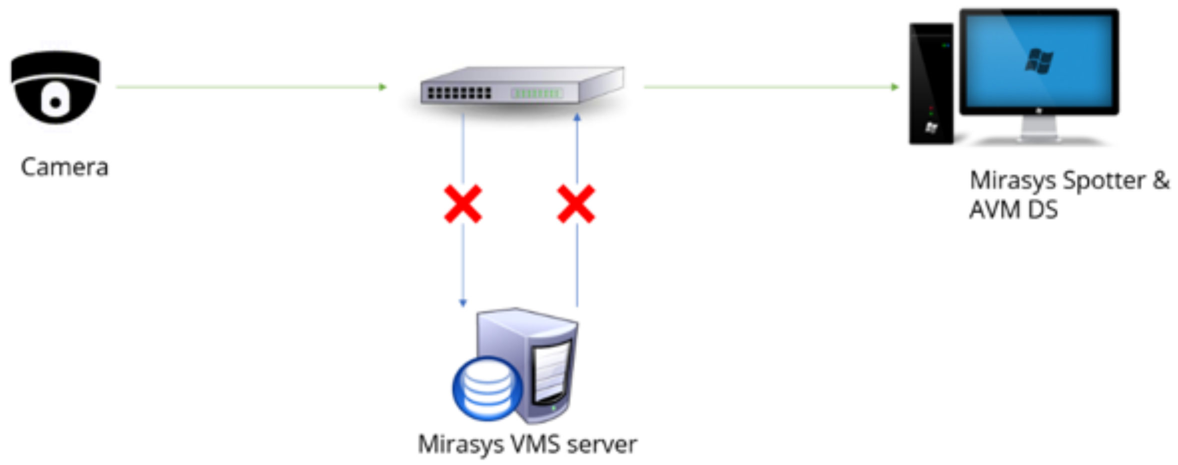
With TruCast, the video stream comes directly from the camera to the viewing client, the Spotter for Windows application.

In a standard streaming scenario, the stream to the client comes from the VMS Server.

Stream from the server to the client



Stream from the camera directly to the client



It is possible to get the direct stream from the camera to the client when the VMS Server connection is OK. This can be useful if users want to optimize network utilization.

Supported Cameras

TruCast requires a separate camera capture driver for the client.

Currently, drivers exist for the following camera manufacturers:

- Acti
- Axis
- Bosch
- Dahua
- Hikvision
- Lilin
- Samsung
- Sony
- Stanley
- ONVIF

Use the ONVIF TruCast driver for cameras that are not on the supported list.

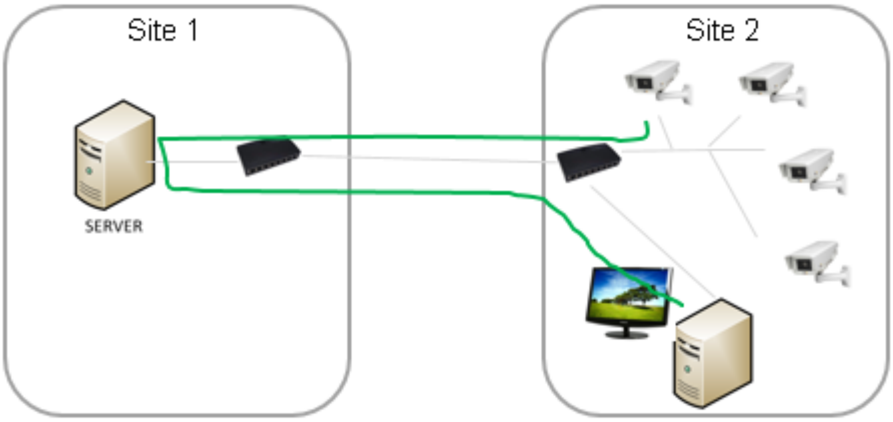
The use of the ONVIF driver requires that the camera is added to the VMS system with the ONVIF driver, not the camera's native driver.

Network Optimization

TruCast can be used to reduce network load in specific scenarios.

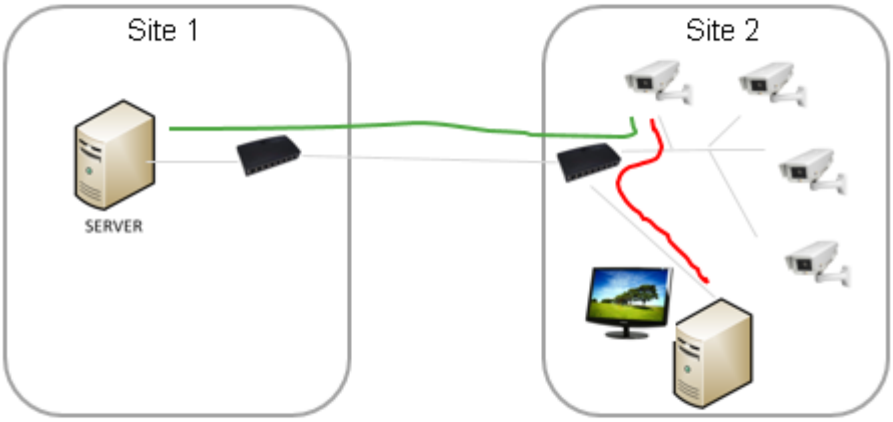
The load reduction mainly occurs when the server is located off-site (remote) and the viewing client is on-site (local to the cameras).

An example scenario 1, we have two sites where the recording is off-site, and the viewing client is on-site. In the following diagram, the viewing is done without TruCast, and the video goes first to the server and then from the server to the viewing client.



In this solution, the traffic between the two sites is increased.

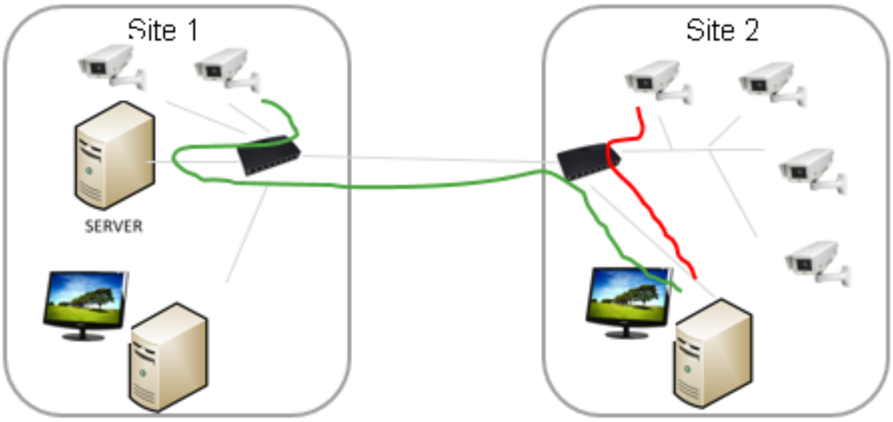
If the stream is consumed directly from the camera with TruCast, the traffic between the two sites is reduced.



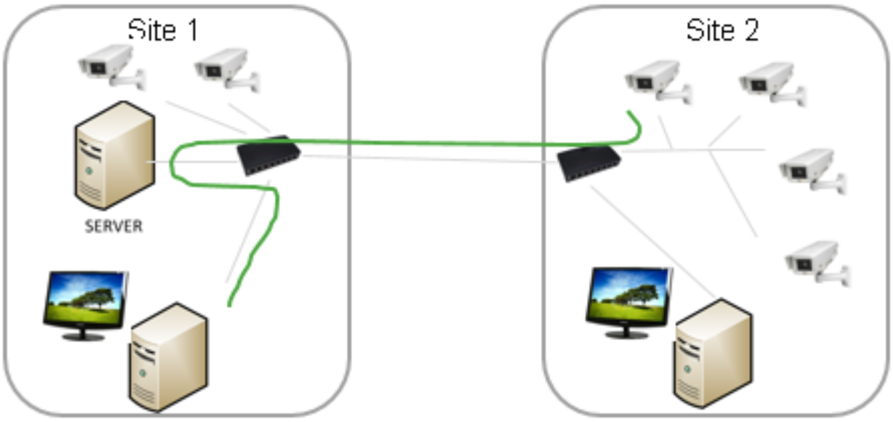
An example scenario 2, there are cameras on two sites and viewing clients on two sites.

For the Site 2 user, the use of TruCast makes more sense for the on-site cameras.

The user can choose to use TruCast for all cameras or only for the on-site cameras.



For the Site 1 user, the use of TruCast only reduces the amount of traffic from the server to the nearest network connection.



Users have complete control over which cameras are using TruCast and which cameras are viewed typically.

The setting is memorized for each camera and each user and saved to Spotter layouts.

Multistreaming and TruCast for Network Optimization and Storage

Since it is also possible to use a different stream for TruCast than the recording stream, this should be considered when planning the network capacity.

For example, users can choose to view live images with TruCast at a higher framerate (for example, 25 fps) and always record at a lower framerate (for example, eight fps).

This reduces the storage and network requirements considerably.

Impact of TruCast on Image Delay

Since the TruCast stream does not travel to the VMS Server and back, the delay from the camera to the client is slightly smaller, but the difference to the stream received from the server is not large, only some milliseconds.

The difference in the two-stream modes is complicated to observe in real life.

Features Not Supported in TruCast Streaming

TruCast does not support PTZ control or Audio

Also, currently, TruCast supports only live images. Playback (recorded images) is currently always received from the server.

Licenses

TruCast requires the VMS license to have the TruCast feature and the TruCast client driver identifiers used.

These TruCast driver licenses, and the TruCast feature, are always enabled in the Mirasys V9 product version.

Multiple Viewers

Since each TruCast-viewer opens an individual new stream from the camera to the client, users should trial how many streams can reliably be opened from the cameras they are using. In practice, 3-5 streams typically work ok.

Installing Client Drivers

Before using TruCast, the necessary client drivers need to be installed with the System Manager application if they have not been installed with the original system installation.

The client driver packages are available in the whole setup package from Mirasys. They are named with the ".sdi" filename extension.

These drivers are installed on the System Manager application's first page, "Install client driver."

The new drivers can be added by pressing the "Install new client driver" button and choosing the SDI packages.

After this, click the "OK" button.

After installing the drivers, they still need to be downloaded to the viewing Spotter clients. This is done when Spotter is restarted from the desktop.

After Spotter has downloaded the new drivers, the system is ready for TruCast use.

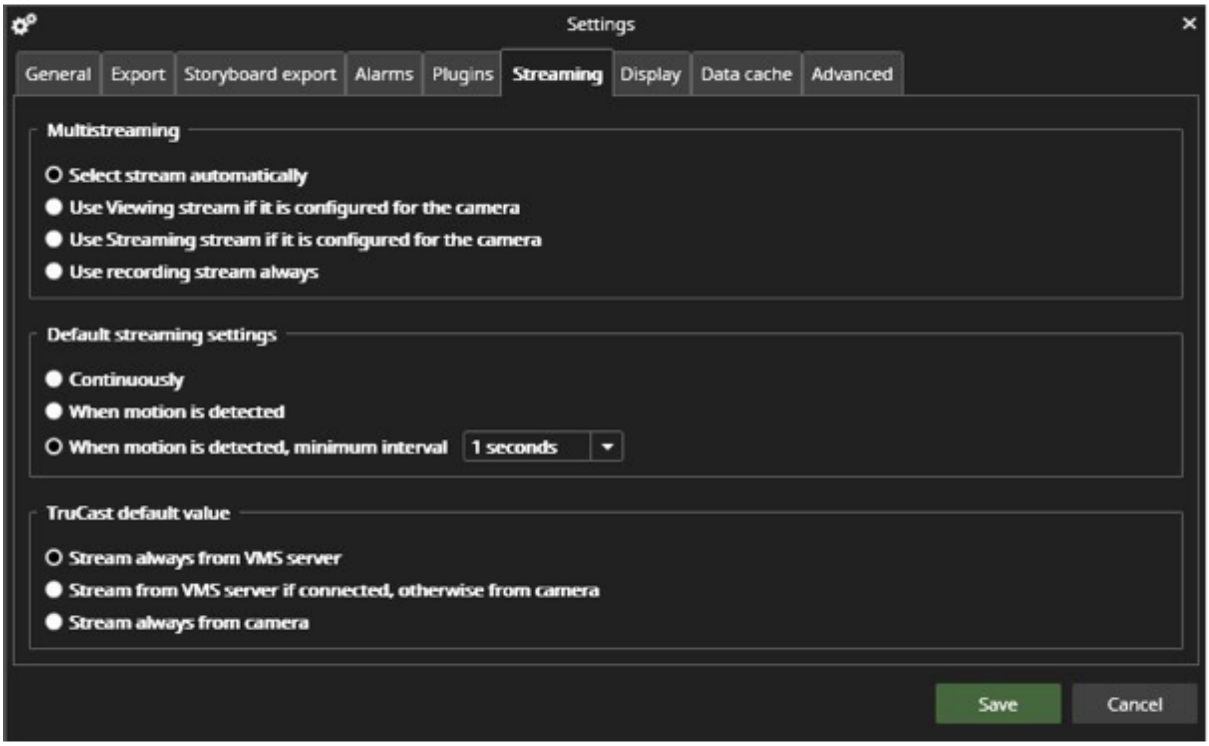
Please note that only those cameras which' client driver was installed will appear as TruCast enabled.

Configuring multi-streaming

TruCast can use any stream from the camera, the Recording, Live viewing or Remote streams.

The multi-streaming is enabled and configured typically in System Manager – cameras.

In the Spotter client settings – streaming – multi-streaming, the user can choose which one of the streams is used for viewing. The same setting is used for standard and TruCast viewing.



Multistreaming

○ Select stream automatically
● Use Viewing stream if it is configured for the camera
● Use Streaming stream if it is configured for the camera
● Use recording stream always

Default streaming settings

● Continuously
● When motion is detected
○ When motion is detected, minimum interval 1 seconds

TruCast default value

○ Stream always from VMS server
● Stream from VMS server if connected, otherwise from camera
● Stream always from camera

TruCast Default Setting

The default setting for all cameras that have not been used for TruCast before can be defined in Spotter settings – streaming – TruCast default value.

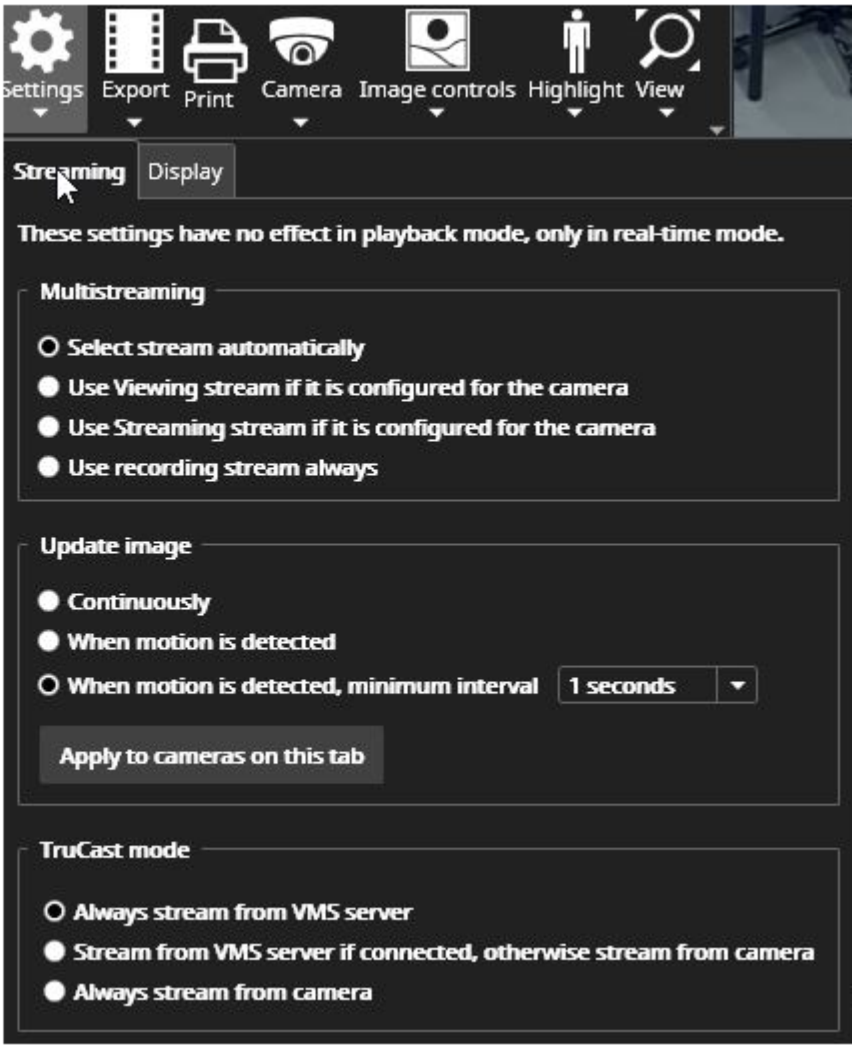
The possible values are

- Always stream from the VMS Server
- Stream from the VMS Server normally, but switch to TruCast if the connection to the server is lost
- Always stream using TruCast

Using TruCast

The user can see the cameras that have TruCast capability from the camera toolbar – settings.

For those cameras that have TruCast the setting is available.



These settings have no effect in playback mode, only in real-time mode.

Multistreaming

○ Select stream automatically
● Use Viewing stream if it is configured for the camera
● Use Streaming stream if it is configured for the camera
● Use recording stream always

Update image

● Continuously
● When motion is detected
○ When motion is detected, minimum interval 1 seconds

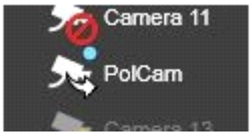
Apply to cameras on this tab

TruCast mode

○ Always stream from VMS server
● Stream from VMS server if connected, otherwise stream from camera
● Always stream from camera

For cameras that do not have TruCast, the lower part of the dialogue is disabled.

The setting is memorized for each camera separately.



When TruCast is active, there is a small arrow displayed on top of the camera in the device tree.

Failover Servers

! If you need to failover also the VCA channels, the failover server must contain the correct amount of the activated VCA channels.

Mirasys VMS supports failover video servers as a Mirasys VMS option.

Failover servers are VMS Servers on a passive standby until the system recognizes that one of the active video recording VMS Servers has broken down; at this point, a failover server takes the place of the broken server.

The failed server can be repaired and replaced as a new failover server, while the failover server that took its place can continue operating as an active server.

***Note**: When a failover server takes the place of an active server, any Spotter plugins (such as Grafana or List Management Application) that are not built-in are not included in the switch and must be re-installed manually after a server restore.*

Recording and failover servers should be of a similar hardware setup and share drive letter assignments and version numbers.

Analogue cameras connected to a server's capture card will not be transferred to the failover server. Only previously assigned IP cameras are reassigned during the switch.

Failover Functionality

When adding a new server into the system, the administrator can select whether the added server is a standard server or failover server.

There can be any number of failover servers (0-n).

If the server is the standard server, the administrator can choose if that particular server will be added to the failover monitoring, i.e., in case of server failure (hardware or software), this server will migrate to the available failover server.

It is important to note that the Master server needs to be installed on hardware separate from those operating with recording licenses or failover licenses.

The minimum hardware setup consists of three servers: one Master Server, one video recording VMS Server, and one standby failover server.

Failover migration will be triggered in the following conditions:

- The Master Server has lost the connection to a VMS Server, and the timeout set by the administrator has been reached
- A VMS Server has informed the Master Server that connection to all the material disks (recording storage) on the server has failed
    - Manual data recovery from server hard drives can be attempted if the disks are still functional
- A server's Watchdog service has informed the Master Server that it cannot initialize the recording service

A recording is continuous after the failover server has taken over to keep the system operational. The only exception is the timeout time between disconnect and failover trigger. The administrator configures this.

After a failover server has assumed the recording role of a failed server, a system backup will automatically be created to set a new baseline.

During the failover restore process and the following system backup:

- Users cannot perform manual backup operations
- Any following broken servers are added to a failover queue

The failover queue is handled after the failover restore has been completed.

Failover summary since V9.5.0

In V9.5.0 VMS, failover functionality was renewed to work quicker than before. It can be triggered manually. In the same version, failback functionality and material copying from failover server to recorder after failback was also implemented.

Failover log was also added where the user can see all occurred failovers and how those are processing, and the user can also trigger failback and material copying manually.

Description

Failover in V9.5.0 was changed not to use system backup files. Instead, SMServer will store recorder settings with schedules and motion masks to recorder settings cache and uses these settings when doing the failover.
Recorder settings, schedules and masks are requested from the recorder when SMServer makes connection to the recorder.
As a part of the making failover quicker, recorder startup was also optimized to start as quickly as possible.

There are now also smaller network disconnection detection times added. In earlier version the smallest time was 1min, but now there are options for 10s, 20s, 30s, 40s and 50s.

Recorder settings cache

- Recorder settings are cached to folder "C:\Program Files\DVMS\SystemManagement\RecorderSettingsStore"
- Recorder masks are cached to folder "C:\Program Files\DVMS\SystemManagement\RecorderMasksStore"
- Recorder schedules are cached to folder "C:\Program Files\DVMS\SystemManagement\RecorderSchedulesStore"

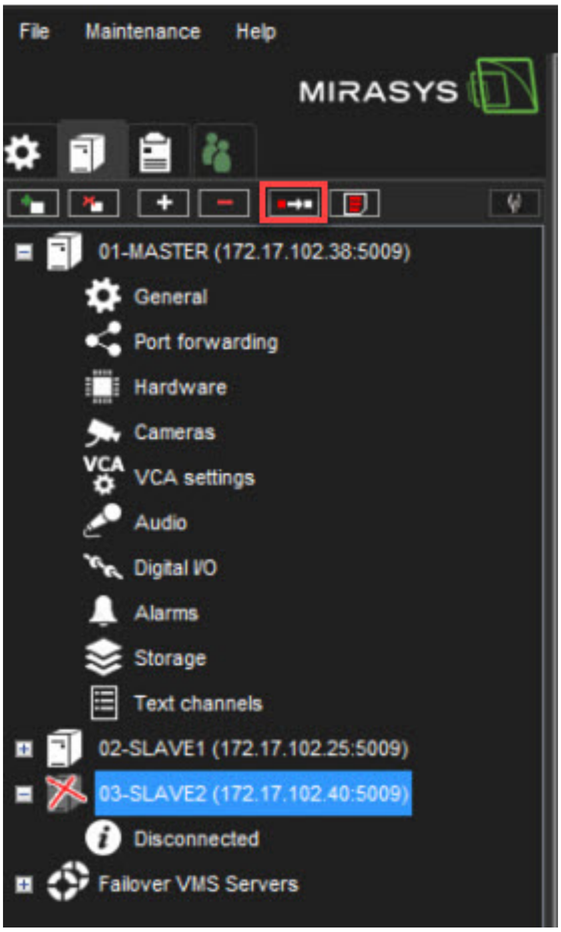
Failover process

- When failover is started (triggered manually by user, by network connection lost or by critical recorder failure), SMServer will do following operation
- Check if there is failover server available that belongs to same failover group as failed recorder and there is connection to the failover server
- Creates failover log entry about the failover
- Get settings, masks and schedules of the failed recorder from recorder settings cache
- Saves failed recorder settings to failover server
- Makes changes to system data that failover server has taken the tasks of the failed server
- Makes changes to the system data that failover server is now acting as normal recorder and failed recorder is in broken state
- Sets failover progress result to failover log
- Sends system change notification to clients

Manual failover triggering

User can trigger manual failover from System Manager UI in recorder settings tab. Manual failover is possible, if

- there is connection to a failover server that belongs to same failover group as the selected recorder
- selected recorder has failover enabled
- User has role that allows to trigger failover manually
- Select the broken VMS server from the list
- Click **Start failover from selected VMS server to the failover server**



Minimum requirements

- **Master server installed on separate PC**

    - The license must contain an automatic backup feature
    - The license must contain one or more failover server
- **1 slave server for recording**
- **1 standby failover server**
- The license must contain at least the same amount of video channels as recording slave server
- Same size material HDD and assigned drive letters

IP camera drivers

Please make sure that failover servers contains the same version drivers, which normal recording servers has

VMS Server roles

VMS Server role FAILOVER

To set a server as a failover server, there has to be a free failover license slot available.

When a server is added as a failover server, the System Manager sets the server to standby mode.

The Failover VMS Servers group shows server connection states and server general settings if the connection is available.

VMS Server role BROKEN

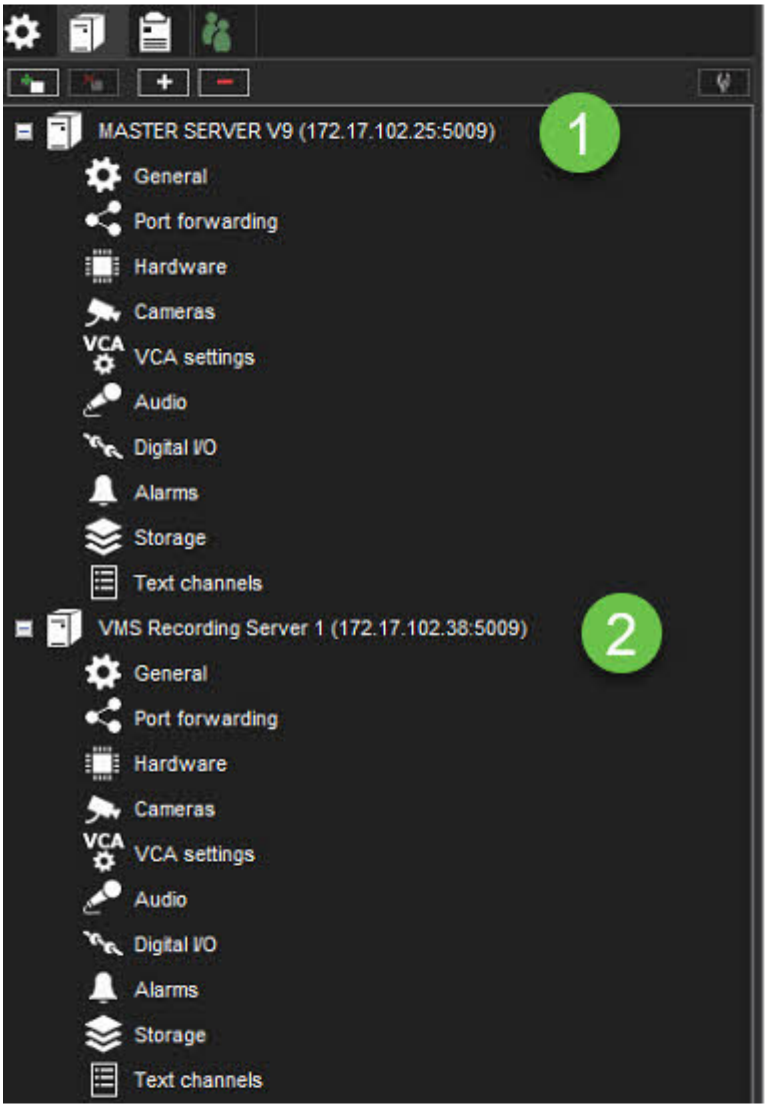
The Broken VMS Servers group displays connection states; the settings on broken servers cannot be changed.

Users can, however, export server logs if there is a connection to a broken server.

To get a broken server that has been replaced by a failover server back into the system, it must first be removed manually and then added again as a new server.

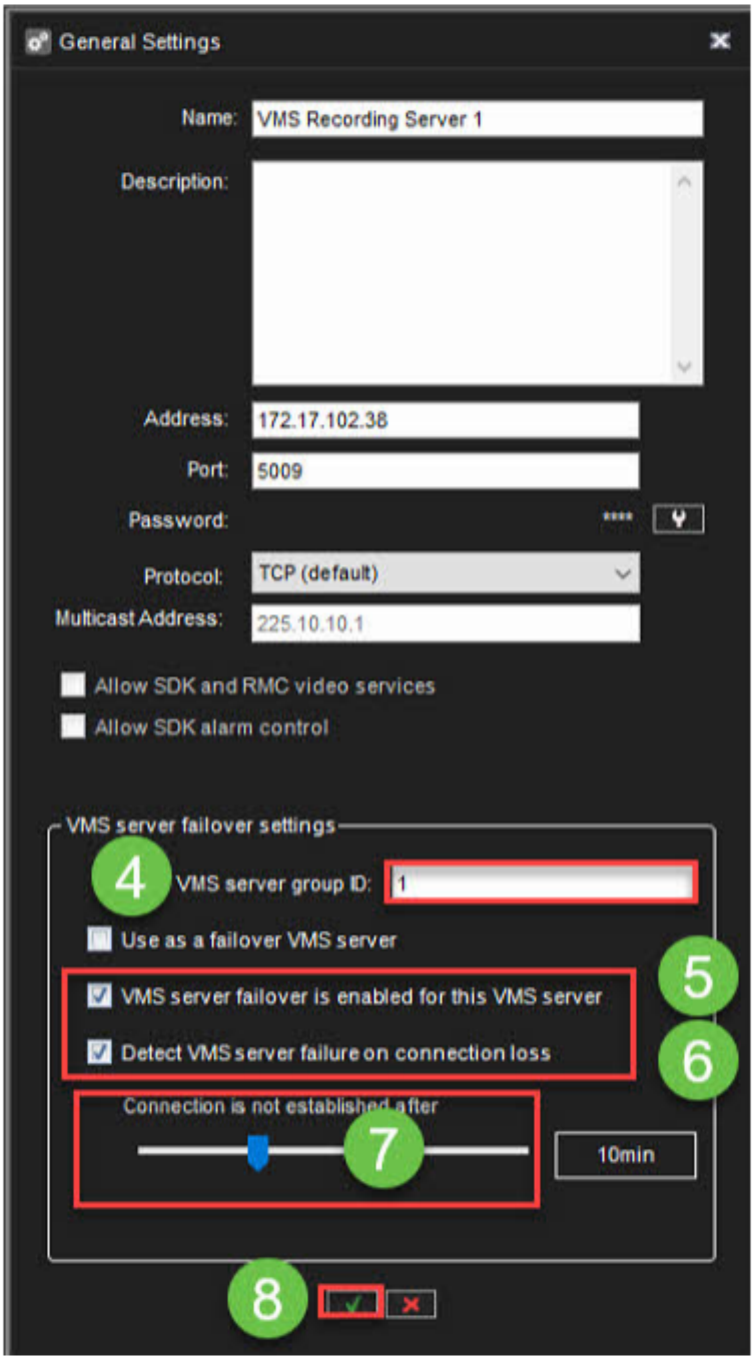
Starting point

The master server and 1 recording slave server were added to the system



Enabling VMS failover server to the recording server

- Open the **VMS Servers** tab
- Select slave server from the list
- Click **General**
- Define **VMS server group ID(default 1)**
- Enable **VMS server failover is enabled for this VMS server**
- Enable **Detect VMS server failure on connection loss**
- Define value **Connection is not established an after**
- Click **OK**



General Settings

Name: VMS Recording Server 1

Description:

Address: 172.17.102.38

Port: 5009

Password: ****

Protocol: TCP (default)

Multicast Address: 225.10.10.1

☐ Allow SDK and RMC video services

☐ Allow SDK alarm control

VMS server failover settings

VMS server group ID: 1

☐ Use as a failover VMS server

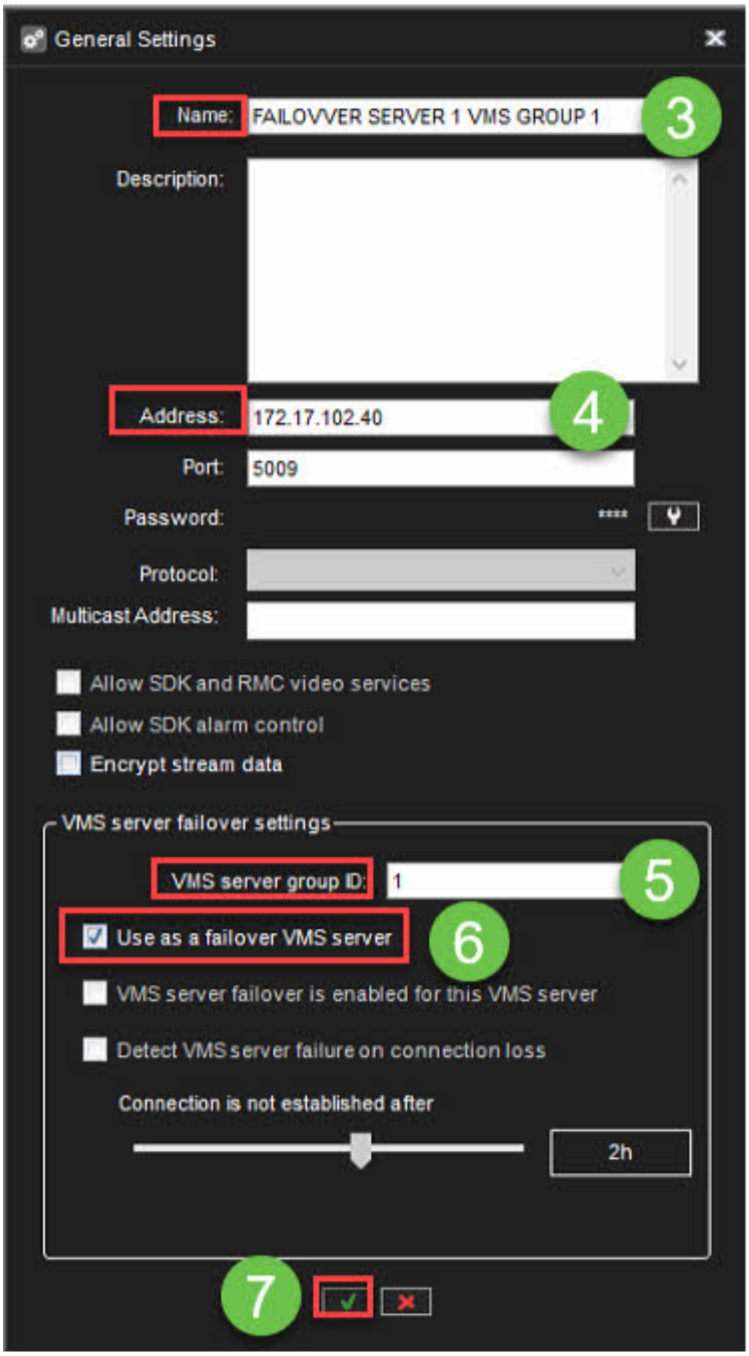
☑ VMS server failover is enabled for this VMS server

☑ Detect VMS server failure on connection loss

Connection is not established after 10min

Adding FAILOVER server

- Open the **VMS Servers** tab
- Click **Add VMS server**
- Set the name for the server
- Set IP address of the server
- Define the **VMS server group ID**
- Enable **Use as a failover VMS server**
- Click **OK**



Name: FAILOVVER SERVER 1 VMS GROUP 1

Description:

Address: 172.17.102.40

Port: 5009

Password: ****

Protocol:

Multicast Address:

□ Allow SDK and RMC video services

□ Allow SDK alarm control

□ Encrypt stream data

VMS server failover settings

VMS server group ID: 1

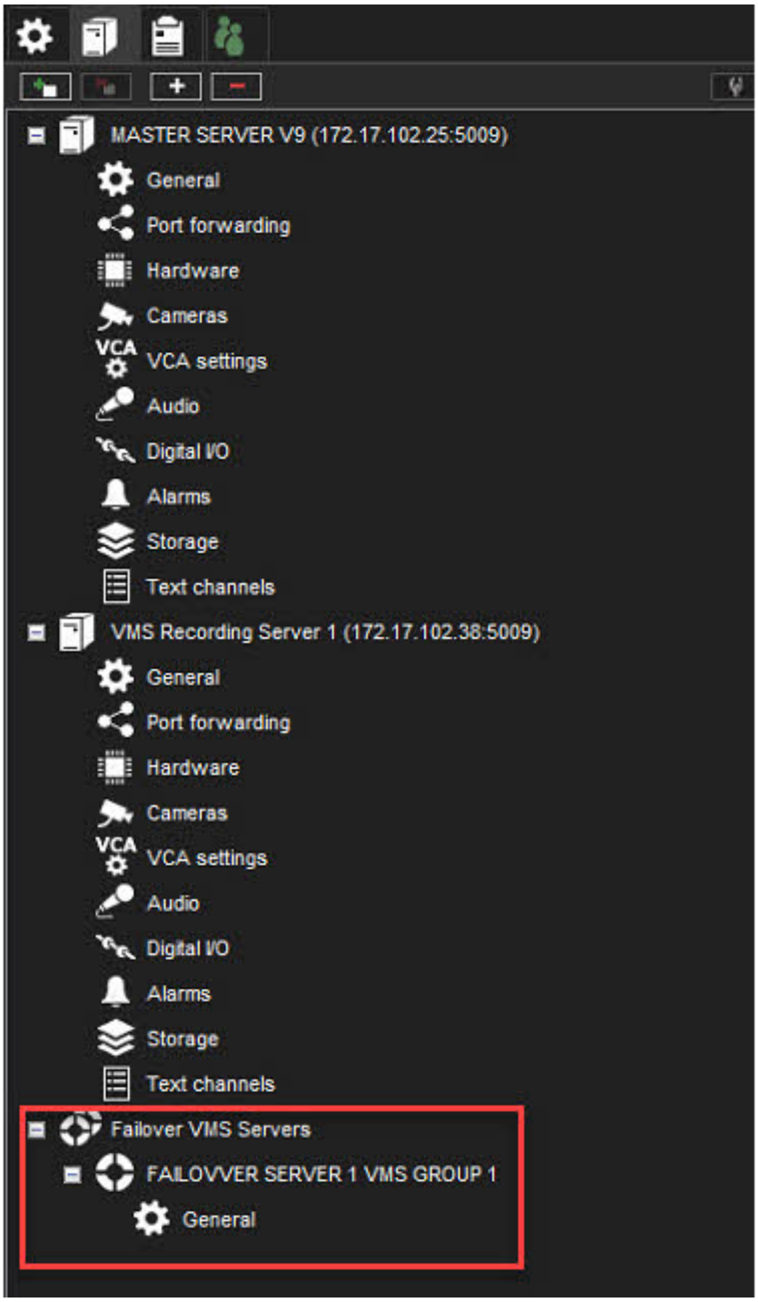
☑ Use as a failover VMS server

□ VMS server failover is enabled for this VMS server

□ Detect VMS server failure on connection loss

Connection is not established after 2h

After the adding, the VMS Server tab shows **Failover VMS Server** line



Failback

Supported from V9.5.0

In V9.5.0 failback can be done either automatically or manually and there is no need to use settings backup to revert the failover.

The Failback uses same functionality as failover, but in reverse order by moving server functionality from failover server back to failed server. Manual failback can be triggered from failover log. Automatic failback will trigger failback when automatic failback is enabled and connection to failed server is restored successfully.

Failback process

When failback is triggered (manually or automatically):

- Check that there is valid failover log entry and the failover state in the log is correct
- Check that failover server is still acting as normal recorder
- Check that failed server is still in broken state
- Check that failover is enabled in the license
- Check that there is no ongoing failback process running for the failed recorder
- Update the failover log that failback is started
- Get failover server recorder settings, configuration files, masks and schedules from recorder settings cache
- Set failed recorder settings
- Mark failover server to act as failover server again and mark failed recorder to be in ok state
- Update the failover log that failback has been performed
- Send system change notification to clients

Manual failback triggering

Failback can be triggered manually from failover log. Manual failback is possible if

- failover has performed successfully
- failback is not in progress or failback is not performed already
- user has role that allows to trigger failover manually

Automatic failback

Automatic failback can be enabled from server general settings when failover is enabled for the server. Automatic failback will not occur if maintenance mode is on.

Automatic failback is triggered when SMServer service connects successfully to failed server. Failback functionality will then get all failover log entries from failover log database for the failed server where failover has been done successfully and failback process has not been done successfully and failback process is not ongoing.

If one or more log entries are found, failback process (described above) is processed.

If there are more than one failover log entry that fulfills the automatic failback requirement, newest log entry is used for failback process.

When the failback process have been successfully done, log entry that was used for failback is updated that failback is done successfully. For other log entries, failback and material copying are marked as done successfully.

Material copying from failover period

Material copy is done from failover server to main server, this task is added to server's processing using DVRFailoverService.

DVRFailoverService has those methods:

- **StartDataCopy** - add new material copy task to server processing queue
- **UpdateClientInfo** - update client information for server in case of connection between server and SMServer was lost to communicate with failover server correctly
- **UpdateFailoverTaskState**s - update material copy state in case of connection between server and SMServer was lost
- Server saves material copy task to database and process those tasks one by one. If some task will be failed, server save last task times and state and continue with other tasks.

What is copied during material copy for a specified time period (start of failover operation and end of failback operation):

- Audio data for all configured audio channels
- Video data for all configured video channels
- Text data for all configured text channels
- Metadata for all configured video and text data channels
- ANPR data for all configured video channels
- Alarms for all configured alarm id's
- Server process each channel listed above one by one and save last received channel time. If connection between servers will be broken or some error will happen, recorder saves last state of material copy task and continue from last unprocessed channel (and last processed channel time).

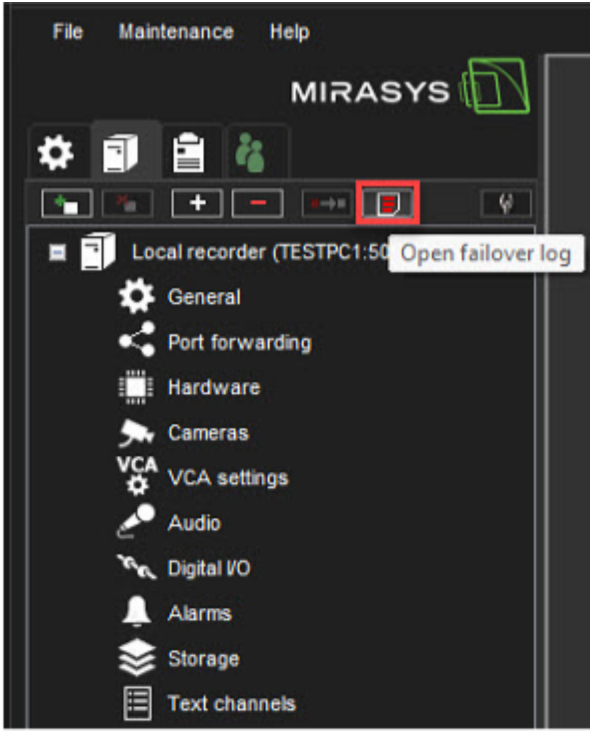
Server use playback functionality for audio, video, text and metadata and ANPR and Alarms search services to get required data for specified time period.

Also, due to Geniune channels security limitations we can't use server as ZpaServer and ZpaClient at the same time, so calllbacks are not working in communication server to server.

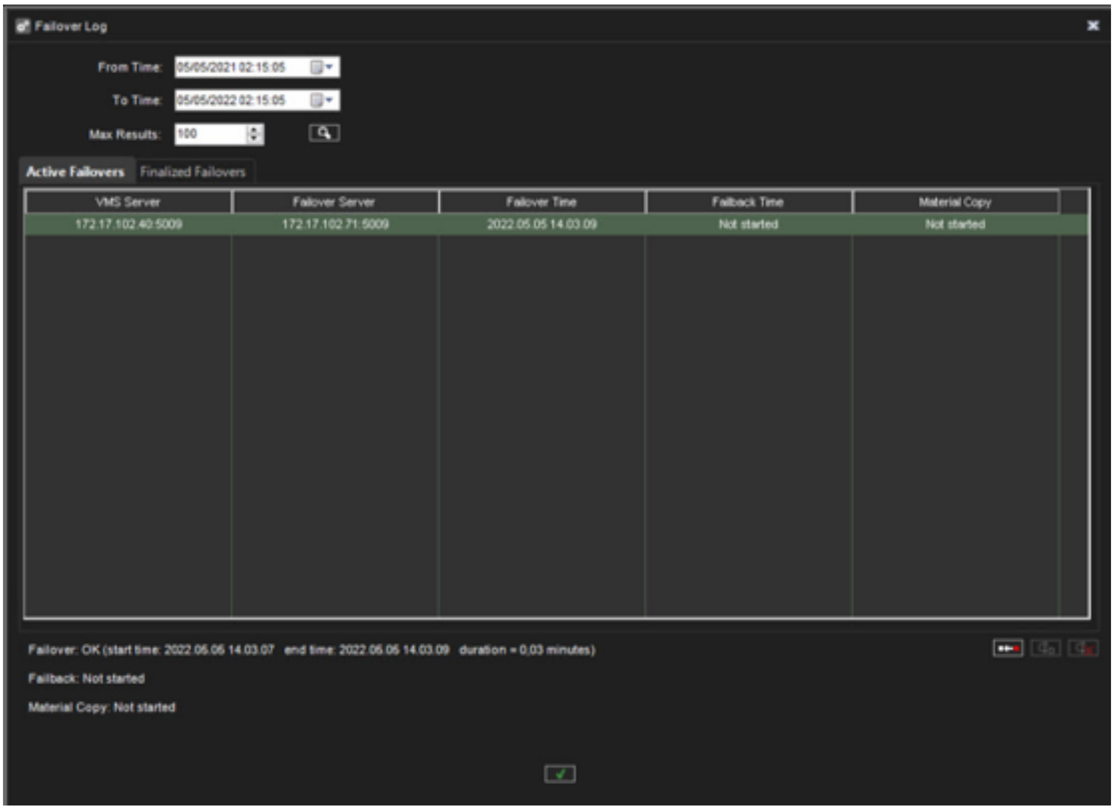
So, ANPR and Alarms search services now have additional methods to get required data without using callbacks.

Failover log

- Click **Open failover log** from the **VMS servers tab**



- The **Failover log** shows **Active Failovers** and **Finalized Failovers**



Failover Log

From Time: 05/05/2021 02:15:05

To Time: 05/05/2022 02:15:05

Max Results: 100

VMS Server	Failover Server	Failover Time	Failback Time	Material Copy
172.17.102.40:5009	172.17.102.71:5009	2022.05.05 14.03.09	Not started	Not started

Failover: OK (start time: 2022.05.05 14.03.07 end time: 2022.05.05 14.03.09 duration = 0,03 minutes)

Failback: Not started

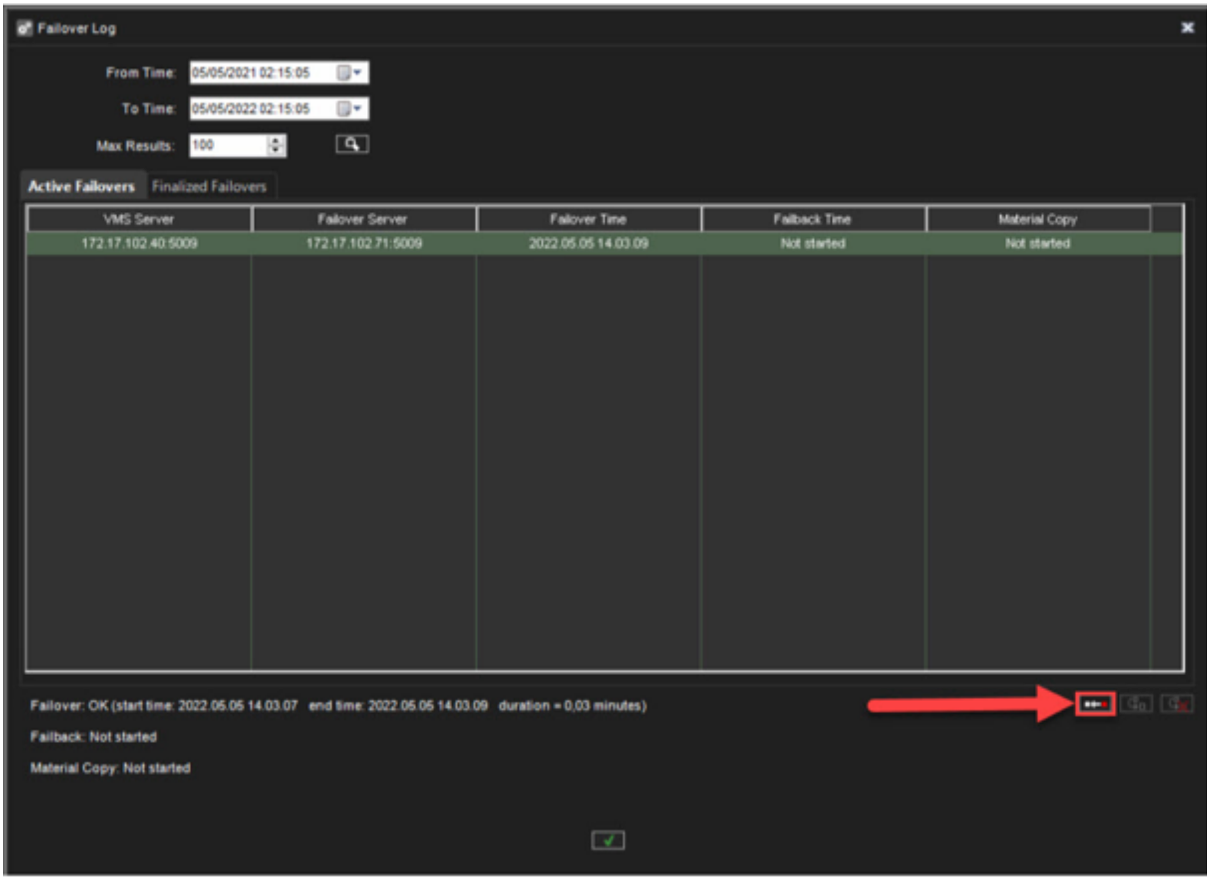
Material Copy: Not started

Start Failback for the selected server

3. Set fixed VMS server to the network with the same IP address

4. Select the server from the list

5. Click **Start failback to the selected server**



From Time: 05/05/2021 02:15:05

To Time: 05/05/2022 02:15:05

Max Results: 100

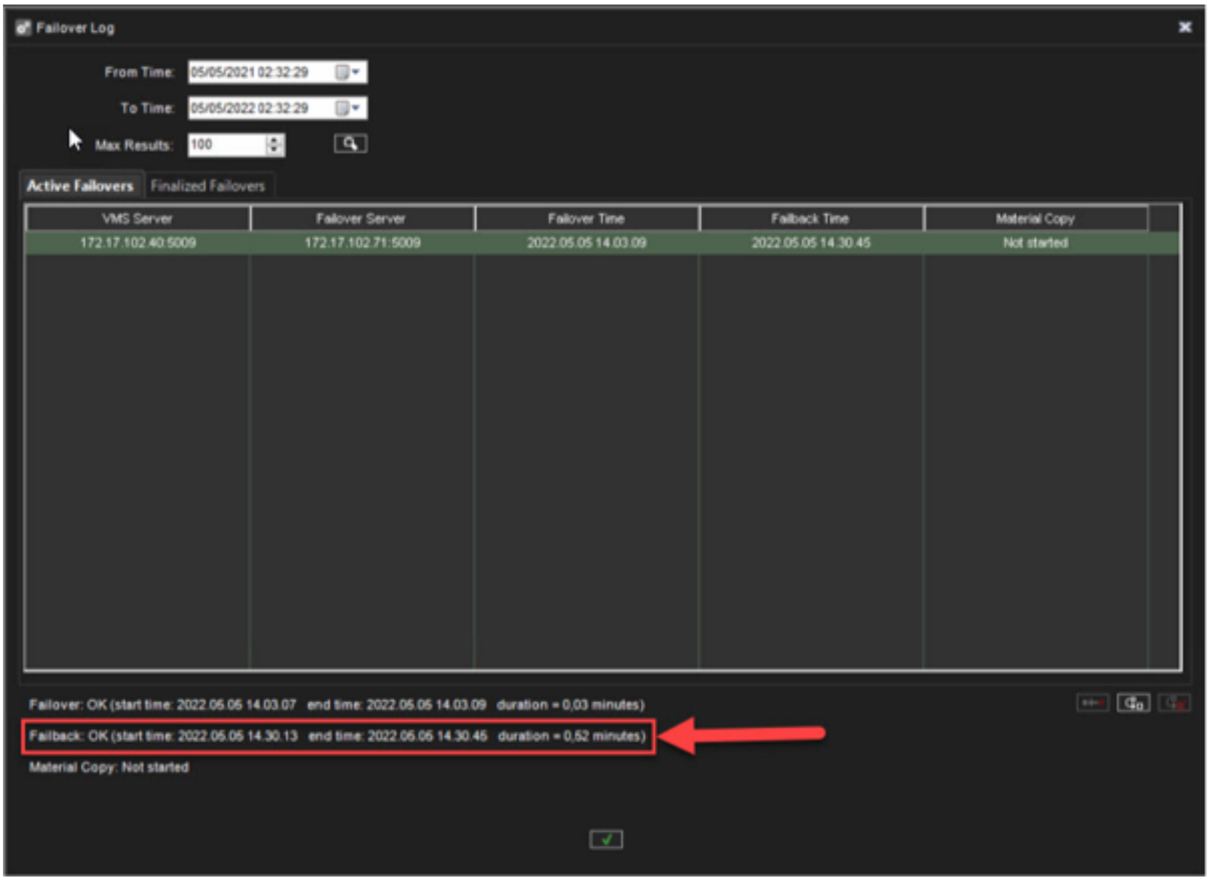
VMS Server	Failover Server	Failover Time	Failback Time	Material Copy
172.17.102.40:5009	172.17.102.71:5009	2022.05.05 14.03.09	Not started	Not started

Failover: OK (start time: 2022.05.05 14.03.07 end time: 2022.05.05 14.03.09 duration = 0,03 minutes)

Failback: Not started

Material Copy: Not started

When the failback is successfully done, Failback OK message with the **start time**, **end time** and **duration** is shown



From Time: 05/05/2021 02:32:29

To Time: 05/05/2022 02:32:29

Max Results: 100

VMS Server	Failover Server	Failover Time	Failback Time	Material Copy
172.17.102.40:5009	172.17.102.71:5009	2022.05.05 14.03.09	2022.05.05 14.30.45	Not started

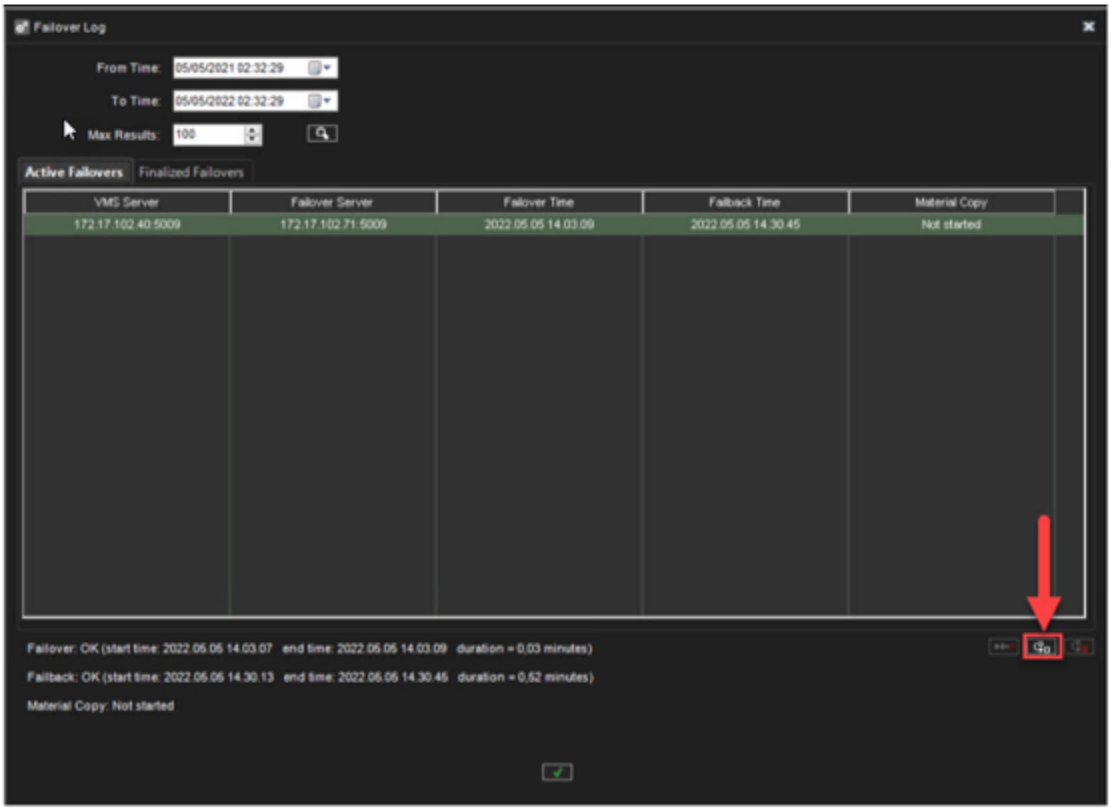
Failover: OK (start time: 2022.06.05 14.03.07   end time: 2022.06.05 14.03.09   duration = 0,03 minutes)

Failback: OK (start time: 2022.06.05 14.30.13   end time: 2022.06.05 14.30.45   duration = 0,52 minutes)

Material Copy: Not started

Start material copying to the selected server

- Select the server from the list
- Select the first material copy, which has not been finalized from the list
- Click **Start material copying to the selected server**



From Time: 05/05/2021 02:32:29

To Time: 05/05/2022 02:32:29

Max Results: 100

VMS Server	Failover Server	Failover Time	Failback Time	Material Copy
172.17.102.40:5009	172.17.102.71:5009	2022.05.05 14.03.09	2022.05.05 14.30.45	Not started

```
Failover: OK (start time: 2022.05.05 14.03.07   end time: 2022.05.05 14.03.09   duration = 0,03 minutes)
Failback: OK (start time: 2022.05.05 14.30.13   end time: 2022.05.05 14.30.45   duration = 0,52 minutes)
Material Copy: Not started
```

Easy LPR

EASY LPR is camera-based LPR detection

Supported since V9.4.0

Supported cameras are:

- Hikvision 7-series LPR cameras
- Axis cameras, which support Vaxtor VaxALPR, version 2.2-20 and AXIS License Plate Verifier version 2.1-0
- Dahua ITC215-PW6M-IRLZF, firmware 2.625

Please check that your Mirasys VMS has at least these driver versions:

- AxisIPCapture64bit_v2.8.1.0
- Dahua IP Capture driver 1.3.1.0 (64bit)
- EHIIPCapture64bit_v2.1.4.0

EASY LPR main features

- Live monitoring from the one camera at the same time
- Plate number search from the one camera at the same time
- Plate number list Management
    - Black list
    - White list
- Importing and exporting plate number lists
- Uploading plate number list to the cameras
- Digital output controlling based on:
    - Other plate detected
    - Black list plate detected
    - White list plate detected

Configuration process

- Configure LPR functionality to the used cameras. Please see the manufacturer website for more information
- Check that license plates are correctly detected in the camera side
- Add cameras to the Mirasys VMS
- Check also camera driver XML file, some cases there is needed to add server details to camera driver XML file, that system can send correct system details to camera

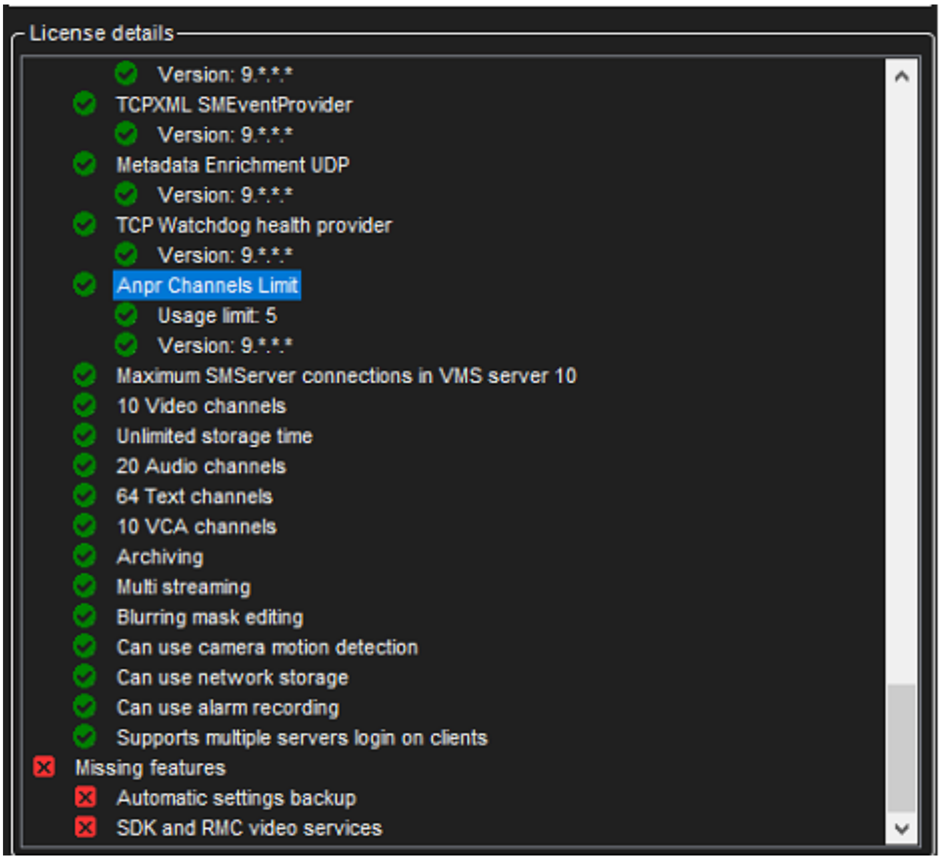
Example NewAxisIPCapture.xml

- We recommend to use **Transport Type: RTP over UDP**
- Check that Mirasys VMS license support LPR cameras
- Enable Easy LPR

Licensing

Mirasys VMS server license defines how many ANPR channels can be added.

The feature name is **Anpr Channels limit** and controllable value name **Usage limit**



License details

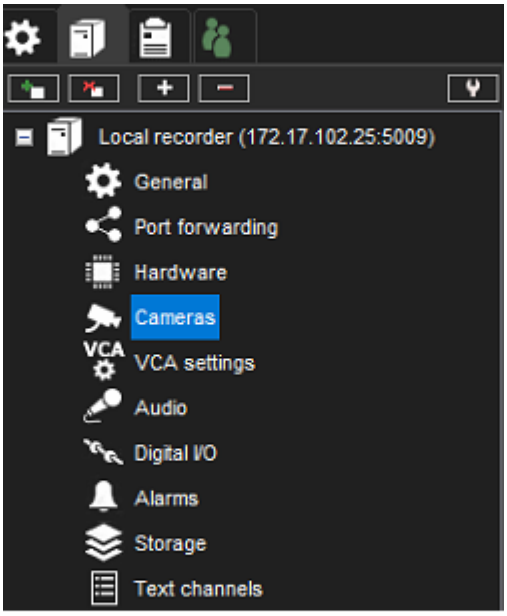
- ✓ Version: 9.*.*.*
- ✓ TCPXML SMEventProvider
  - ✓ Version: 9.*.*.*
- ✓ Metadata Enrichment UDP
  - ✓ Version: 9.*.*.*
- ✓ TCP Watchdog health provider
  - ✓ Version: 9.*.*.*
- ✓ Anpr Channels Limit
  - ✓ Usage limit: 5
  - ✓ Version: 9.*.*.*
- ✓ Maximum SMServer connections in VMS server 10
- ✓ 10 Video channels
- ✓ Unlimited storage time
- ✓ 20 Audio channels
- ✓ 64 Text channels
- ✓ 10 VCA channels
- ✓ Archiving
- ✓ Multi streaming
- ✓ Blurring mask editing
- ✓ Can use camera motion detection
- ✓ Can use network storage
- ✓ Can use alarm recording
- ✓ Supports multiple servers login on clients

☒ Missing features

- ☒ Automatic settings backup
- ☒ SDK and RMC video services

Enabling Easy LPR

- Open **VMS servers**
- Open **Cameras**

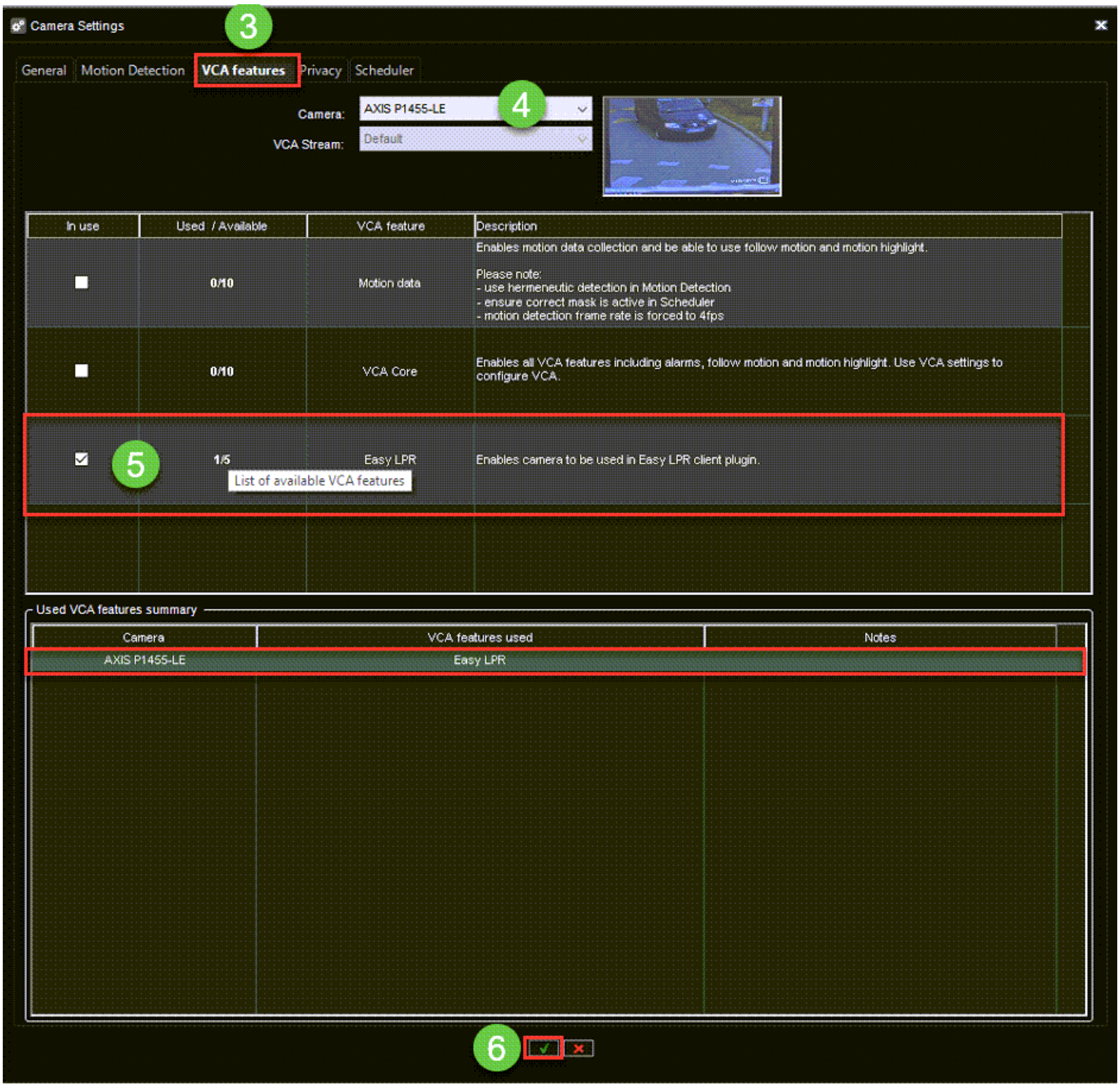


3. Click **VCA features**

4. Select LPR camera

5. Enable **Easy LPR**

6. Click **Save**



Camera Settings

General | Motion Detection | **VCA features** | Privacy | Scheduler

Camera: AXIS P1455-LE

VCA Stream: Default

In use	Used / Available	VCA feature	Description
□	0/10	Motion data	Enables motion data collection and be able to use follow motion and motion highlight. Please note: - use hermeneutic detection in Motion Detection - ensure correct mask is active in Scheduler - motion detection frame rate is forced to 4fps
□	0/10	VCA Core	Enables all VCA features including alarms, follow motion and motion highlight. Use VCA settings to configure VCA.
☑	1/5	Easy LPR	Enables camera to be used in Easy LPR client plugin.

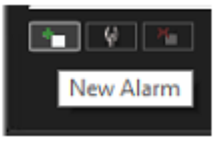
List of available VCA features

Used VCA features summary

Camera	VCA features used	Notes
AXIS P1455-LE	Easy LPR	

Creating an alarm from Easy LPR event

- Go to the **VMS Servers** tab
- Open **Alarms**
- Click **New Alarm**



4. Enter all needed information in the **General** tab

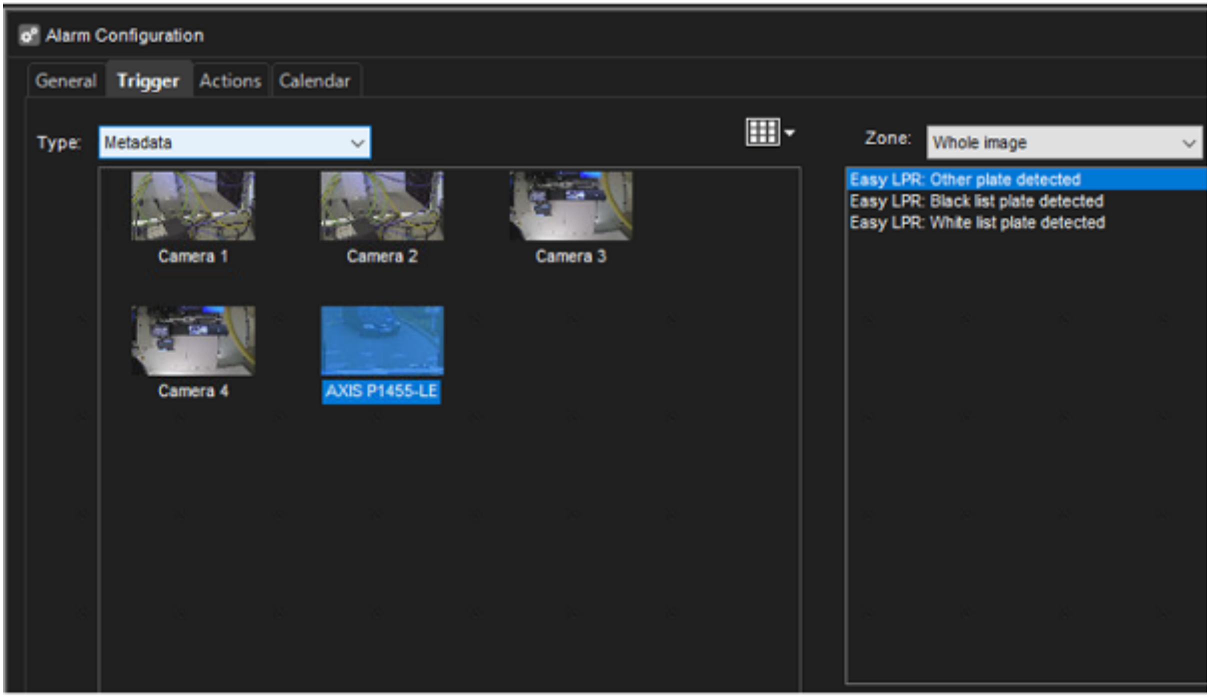
5. Open **Trigger** tab

6. Select trigger type **Metadata**

7. Select LPR camera

8. Select correct event:

- **Easy LPR: Other plate detected**
- **Easy LPR: Black list plate detected**
- **Easy LPR: White list plate detected**



Alarm Configuration

Type: Metadata

Zone: Whole image

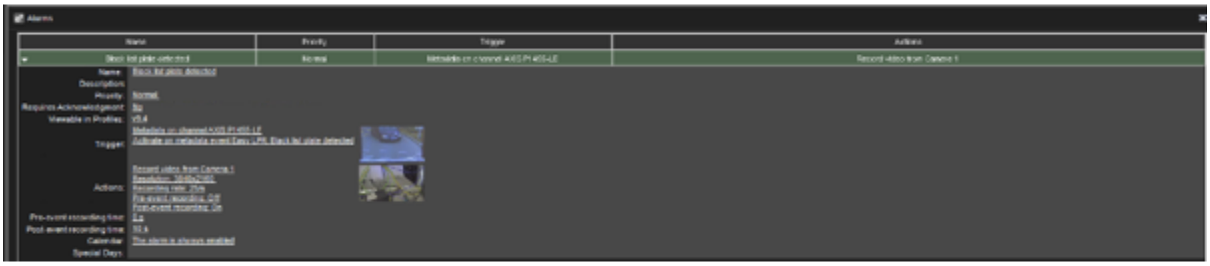
Easy LPR: Other plate detected
Easy LPR: Black list plate detected
Easy LPR: White list plate detected

9. Enter the actions of the alarms

10. Set calendar

11. Check overall view of the alarm

12. Click **OK** to confirm an alarm creation



Alarms

Name	Priority	Trigger	Actions
Black list plate detected	Normal	Metadata on channel AXIS P1455-LE	Record video from Camera 1

Name: Black list plate detected
Description:
Priority: Normal
Requires Acknowledgement: No
Viewable in Profiles: v9.4
Trigger: Metadata on channel AXIS P1455-LE
Activate on metadata event Easy LPR Black list plate detected
Actions: Record video from Camera 1
Resolution: 3840x2160
Recording rate: 25/s
Pre-event recording: Off
Post-event recording: On
Pre-event recording time: 5 s
Post-event recording time: 10 s
Calendar: The alarm is always enabled
Special Days:

AI Guides

Mirasys Face Recognition (FR)

Face Recognition Introduction

Face Recognition (FR) is used to identify a human face. It is used in the VMS System to get events when faces are detected from selected video streams and to detect when specific persons are seen in the video. Together with the Mirasys List Management, this allows you to, for example, create an automatic detection system of a person's access to the premises.

Note that anti-spoofing is not included in version 9.6.

The FR service receives video streams, processes images, detects faces, and sends notifications with detection data to List Management (LM) service for identity and list matching.

Face Recognition service has a separate installer, so it can execute on a separate server or on some VMS server.

Privacy masks

If any client privacy masks are defined for the camera, the FR service draws privacy masks to input images before inference.

- No face can be detected inside the privacy zone.
- Thumbnail images have privacy zones.

FR processing, events, and detection

Devices

Face recognition processing can be done using different hardware. Supported hardware is CPU, Intel GPU, Nvidia GPU, and MAIC (Mirasys AI Card).

FR events

Live FR events are shown in the Smart Recognition plugin in Spotter. FR events can be searched using the Smart Search plugin in Spotter.

Detected face visualization

Detected faces can be visualized in Spotter using the VCA visualization plugin (Highlight menu in camera toolbar).

FR Alarm triggers and configuration

Alarm triggers

An alarm trigger on the VMS server can be created for each identity list that is configured in List Management settings.

FR configuration

FR service can be configured in the System Manager application on the FR settings tab in the **Camera Settings** window.

The FR settings contain information about camera video streams processed by the service. Each stream setting is related to the camera and stream on the recorder. Each FR service can have its own set of limits.

Mirasys License Plate Recognition (LPR)

License Plate Recognition Introduction

License Plate Recognition (LPR) is used to identify a car using its license plate. It is used in the VMS System to get events when license plates are detected from selected video streams and to detect when specific cars are seen in the video. Together with the Mirasys List Management, this allows you to, for example, create an automatic detection system of cars' access to the parking hall.

The LPR service receives video streams, processes images, detects license plates, and sends notifications with detection data to List Management (LM) service for identity and list matching.

License Plate Recognition service has a separate installer, so it can execute on a separate server or on some VMS server.

LPR Privacy masks

If any client privacy masks are defined for the camera, then the LPR service draws privacy masks to input images before doing inference.

- No license plate can be detected inside the privacy zone.
- Thumbnail images have privacy zones.

Country Detection

Country detection is optional, but in some countries, it is recommended to be used: plate number detection accuracy can be improved when the country is known.

Plate number country detection

Plate number detection is available for Eurasia and the Americas.

Country detection is optional. It is useful in countries like Finland, where the letters I and O are the same as numbers 1 and 0. If the country is recognized with high confidence, then country-specific rules can be used to improve plate number detection accuracy.

License plate types

If country detection is enabled, then license plate type can sometimes be detected. License plate type can be undefined or one of these:

- antique
- diplomatic
- export
- military
- provisional
- rental
- taxi
- test
- work

Supported countries in Eurasia (LPR)

Area codes

In some countries, license plates have area codes. If country detection is enabled, then also area code is detected for the following countries:

- Austria
- Germany

- Romania
- Slovenia
- Switzerland

In a special case, a region inside a country can be detected. For example, Åland Islands has its own plate styles, different from those used in other parts of Finland.

> Please note that accuracy vary from country to country.
>
> A plate from **unsupported** countries could be detected as one of the countries listed below.
>
> For example some Tajikistan plates can be detected as Kazakhstan plates.

List of supported countries in Eurasia

- Albania
- Andorra
- Armenia
- Austria
- Azerbaijan
- Belarus
- Belgium
- Bosnia and Herzegovina
- Bulgaria
- Croatia
- Cyprus
- Czech Republic
- Denmark
- Estonia
- Finland (including Åland Islands)
- France
- Georgia
- Germany
- Gibraltar
- Greece
- Hungary
- Iceland
- Ireland
- Isle of Man

- Italy
- Kazakhstan
- Latvia
- Liechtenstein
- Lithuania
- Luxembourg
- Malta
- Moldova
- Monaco
- Montenegro
- Netherlands
- North Macedonia
- Norway
- Poland
- Portugal
- Romania
- Russia
- San Marino
- Serbia
- Slovakia
- Slovenia
- Spain
- Sweden
- Switzerland
- Turkey
- Ukraine
- United Kingdom
- Vatican

Supported countries in the Americas (LPR)

> Please note that accuracy vary from country to country.
>
> A plate from **unsupported** countries could be detected as one of the countries listed below.

Countries and states

The countries/states listed below are supported.

- Argentina
- Bolivia
- Brazil (old and new plate styles)
- Canada
  - Alberta
  - British Columbia
  - Manitoba
  - Ontario
  - Quebec
  - Saskatchewan
- Chile
- Colombia
- Mexico
- Paraguay
- Peru
- United States
  - Alabama
  - Alaska
  - Arizona
  - Arkansas
  - California
  - Colorado
  - Connecticut
  - Delaware
  - District of Columbia
  - Florida
  - Georgia
  - Hawaii
  - Idaho
  - Illinois
  - Indiana
  - Iowa
  - Kansas
  - Kentucky
  - Louisiana
  - Maine
  - Maryland
  - Massachusetts
  - Michigan
  - Minnesota
  - Mississippi
  - Missouri
  - Montana

    - Nebraska
    - Nevada
    - New Hampshire
    - New Jersey
    - New Mexico
    - New York
    - North Carolina
    - North Dakota
    - Ohio
    - Oklahoma
    - Oregon
    - Pennsylvania
    - Rhode Island
    - South Carolina
    - South Dakota
    - Tennessee
    - Texas
    - Utah
    - Vermont
    - Virginia
    - Washington
    - West Virginia
    - Wisconsin
    - Wyoming
- Uruguay
- Venezuela

LPR processing, events, and detection

Devices

License plate recognition processing can be done using different hardware. Supported hardware is CPU, Intel GPU, Nvidia GPU, and MAIC (Mirasys AI Card).

LPR events

Live LPR events are shown in the Smart Recognition plugin in Spotter. LPR events can be searched using the Smart Search Plugin in Spotter.

Detected license plate visualization

Detected license plates can be visualized in Spotter using the VCA visualization plugin (Highlight menu in camera toolbar).

LPR Alarm triggers and configuration

Alarm triggers

An alarm trigger on the VMS server can be created for each identity list that is configured in List Management settings.

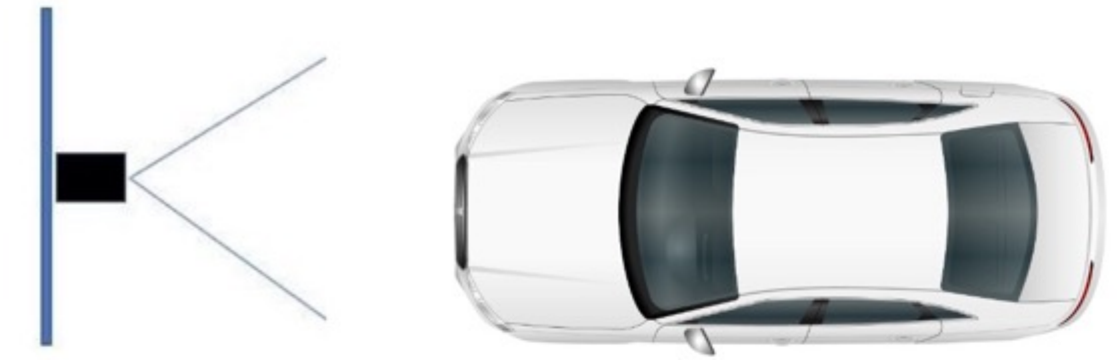
LPR configuration

LPR service can be configured in the System Manager application on the LPR settings tab in the **Camera Settings** window.

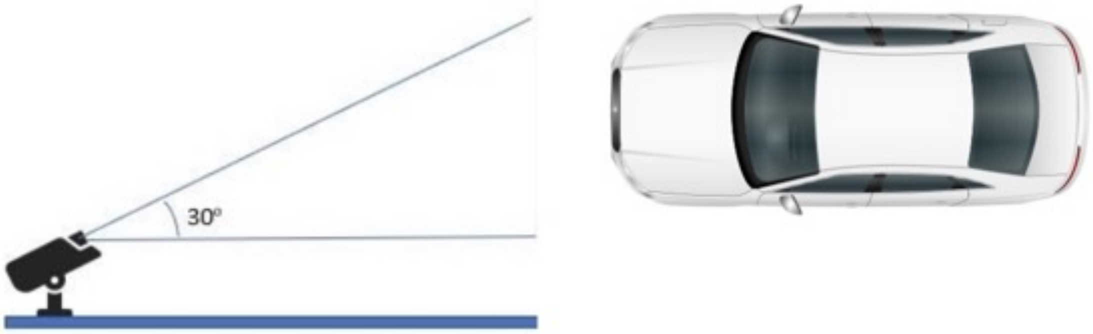
The LPR settings contain information about camera video streams processed by the service. Each stream setting is related to the camera and stream on the recorder. Each LPR service can have its own set of limits.

LPR Camera Installation tips

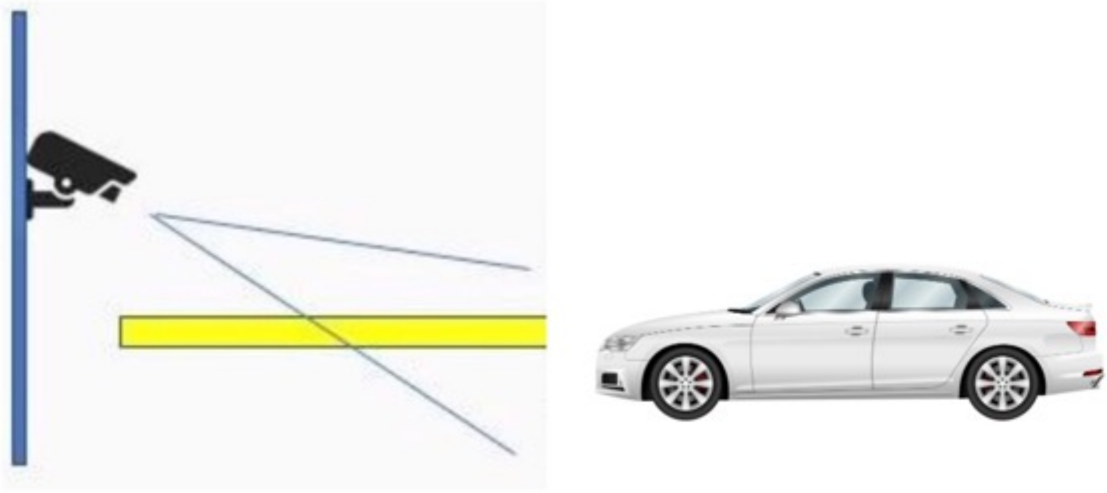
It is recommended to install the camera in the center of the vehicle



If the camera is installed on the side of the road or lane, the angle should not exceed 30 degrees.



The camera should be installed higher than the vehicle headlights so that the vehicle's headlights don't point directly at the camera



Ensure the license plate width is at least 120 pixels and height at least 50 pixels

Height at least 50 pixels

Width at least 120 pixels

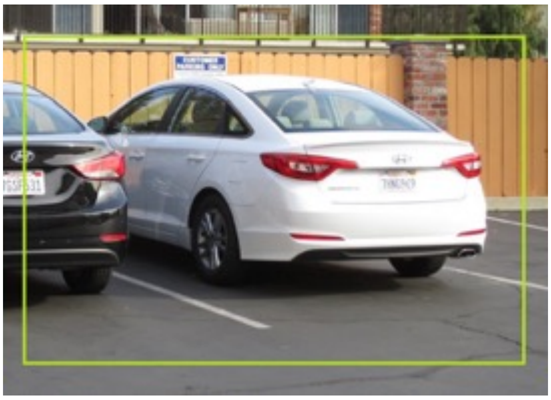
License plate tilt angle must be within +/- 10 degrees

LPR settings in the System Manager application

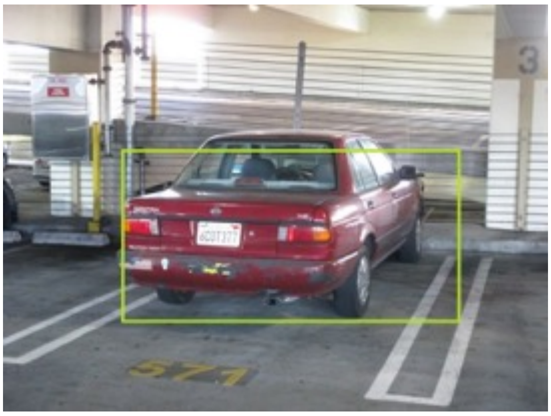
Ensure the correct region (Americas / Eurasia) is selected.

Setting the region of interest

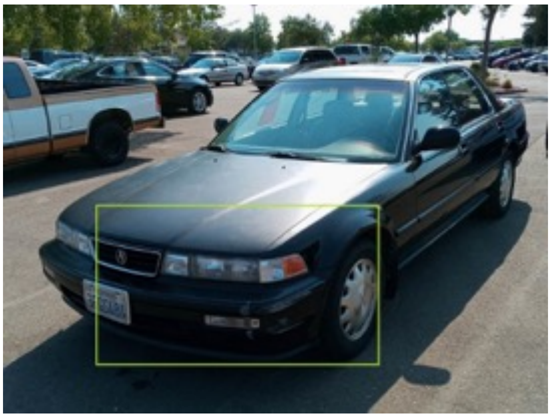
Region of interest is used to define where detection will find license plates.



Leave some margin to the region of interest to not detect partially visible plates.



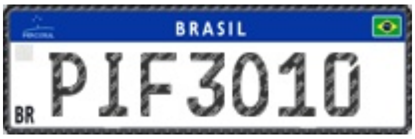
The whole license plate is inside the region of interest, and the plate is detected.



The license plate is not completely inside the region of interest, and the plate is not detected.

Enabling country recognition

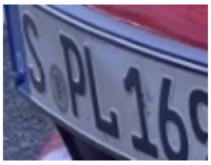
In many countries letter **O** is similar to the number **0**, and the letter **I** looks the same as the number **1**. Enabling country detection improves detection accuracy in these cases.



For example, the format for Brazil plate number is “abc1d23”.

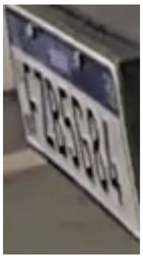
Common problems and solutions

Incomplete license plate



Solution: Don’t set the region of interest too close to image borders.

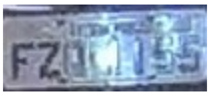
View angle makes plate numbers unreadable



Solution 1: Move the camera to a better place.

Solution 2: Set the region of interest so that the plate is detected when it is visible from better angle.

Other vehicles headlights reflect from license plate



Solution 1: Move the camera to a better place.

Solution 2: Set the region of interest so that the plate is detected when other vehicles' headlights don't point to the license plate direction.

The license plate is too small

Solution 1: Move the camera to a better place or zoom in.

Solution 2: Set the region of interest so that the plate is detected when the vehicle is nearer to the camera.

Solution 3: Increase the minimum plate height value in LPR settings so that small plate detections are ignored.

The license plate is blurry

Solution 1: Adjust sharpness and increase shutter speed in the camera's settings.

Solution 2: Increase the lighting of the area.

The license plate is overexposed

Solution 1: Adjust camera's image settings.

Solution 2: Check the camera installation location and move it higher so that headlights doesn't reflect from the plate.

Easy LPR Guide

EASY LPR is camera-based LPR detection. Supported cameras are:

- Hikvision 7-series LPR cameras
- Axis cameras, which support Vaxtor VaxALPR, version 2.2-20 and AXIS License Plate Verifier version 2.1-0
- Dahua ITC215-PW6M-IRLZF, firmware 2.625

Please check that your Mirasys VMS has at least these driver versions:

- AxisIPCapture64bit_v2.8.1.0
- Dahua IP Capture driver 1.3.1.0 (64bit)
- EHIIPCapture64bit_v2.1.4.0

EASY LPR main features

- Live monitoring from the one camera at the same time
- Plate number search from the one camera at the same time
- Plate number list Management
  - Black list
  - White list
- Importing and exporting plate number lists
- Uploading plate number list to the cameras
- Digital output controlling based on:
  - Other plate detected
  - Black list plate detected
  - White list plate detected

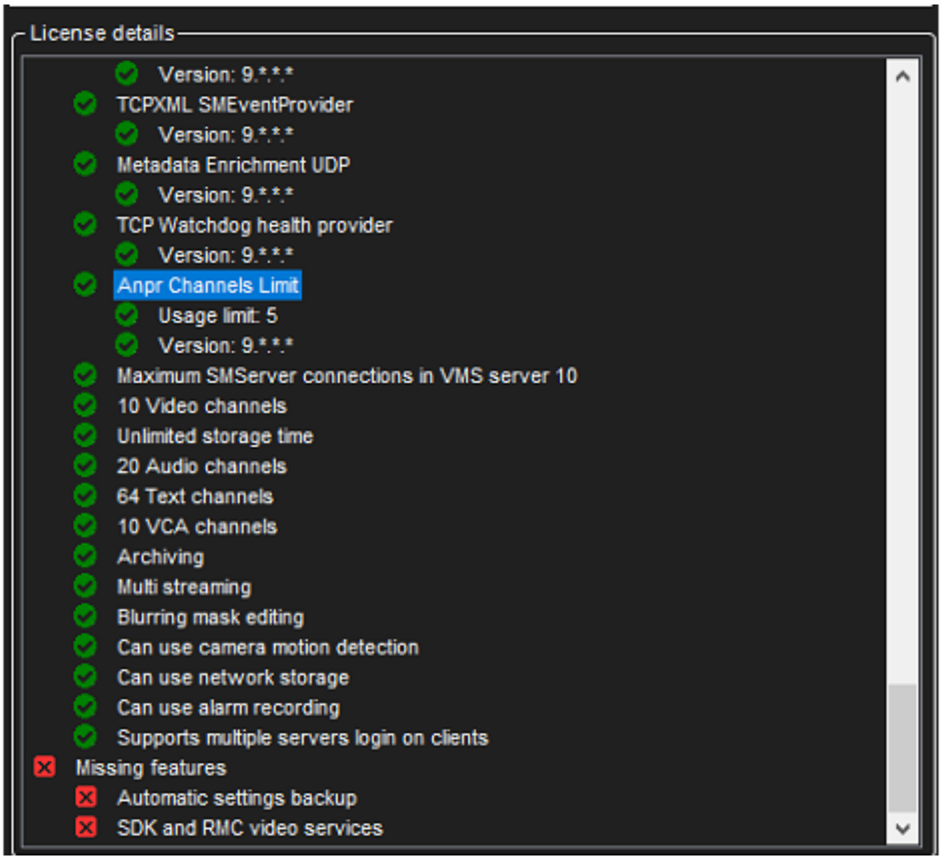
Easy LPR Configuration process

- Configure LPR functionality to the used cameras. Please see the manufacturer website for more information
- Check that license plates are correctly detected in the camera side
- Add cameras to the Mirasys VMS
- Check that Mirasys VMS license support LPR cameras
- Enable Easy LPR

Easy LPR Licensing

Mirasys VMS server license defines how many ANPR channels can be added.

The feature name is **Anpr Channels limit** and controllable value name **Usage limit**

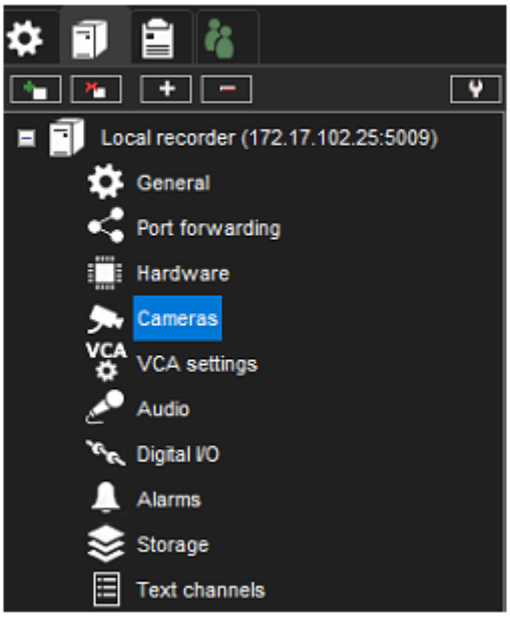


License details

```
        ✓ Version: 9.*.*
    ✓ TCPXML SMEventProvider
        ✓ Version: 9.*.*
    ✓ Metadata Enrichment UDP
        ✓ Version: 9.*.*
    ✓ TCP Watchdog health provider
        ✓ Version: 9.*.*
    ✓ Anpr Channels Limit
        ✓ Usage limit: 5
        ✓ Version: 9.*.*
    ✓ Maximum SMServer connections in VMS server 10
    ✓ 10 Video channels
    ✓ Unlimited storage time
    ✓ 20 Audio channels
    ✓ 64 Text channels
    ✓ 10 VCA channels
    ✓ Archiving
    ✓ Multi streaming
    ✓ Blurring mask editing
    ✓ Can use camera motion detection
    ✓ Can use network storage
    ✓ Can use alarm recording
    ✓ Supports multiple servers login on clients
☒ Missing features
    ☒ Automatic settings backup
    ☒ SDK and RMC video services
```

How to enable Easy LPR

- Open **VMS servers**
- Open **Cameras**

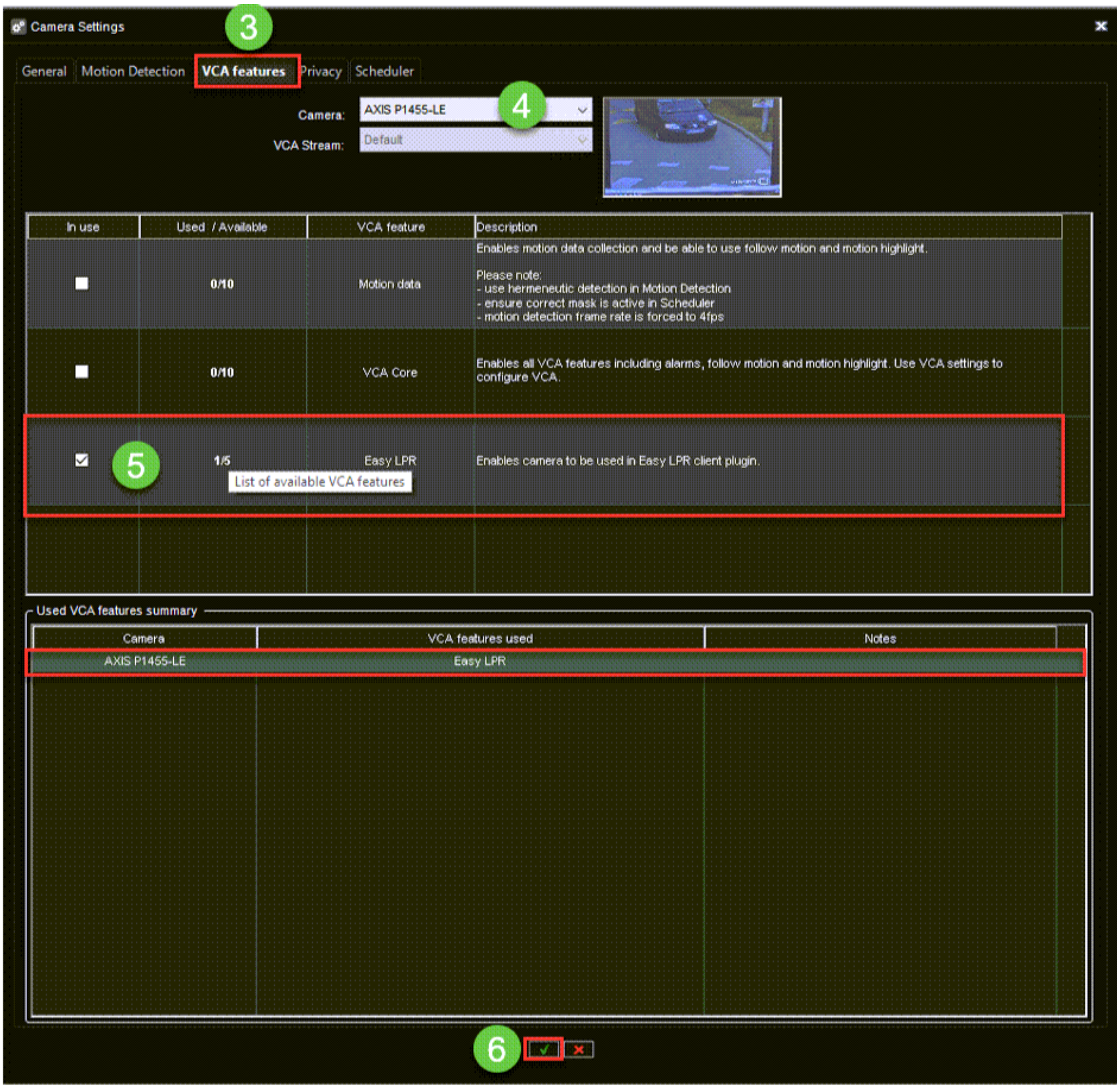


3. Click **VCA features**

4. Select LPR camera

5. Enable **Easy LPR**

6. Click **Save**



Camera: AXIS P1455-LE

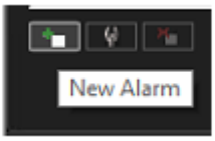
VCA Stream: Default

In use	Used / Available	VCA feature	Description
□	0/10	Motion data	Enables motion data collection and be able to use follow motion and motion highlight. Please note: - use hermeneutic detection in Motion Detection - ensure correct mask is active in Scheduler - motion detection frame rate is forced to 4fps
□	0/10	VCA Core	Enables all VCA features including alarms, follow motion and motion highlight. Use VCA settings to configure VCA.
☑	1/5	Easy LPR	Enables camera to be used in Easy LPR client plugin.

Camera	VCA features used	Notes
AXIS P1455-LE	Easy LPR	

Create an alarm from an Easy LPR event

1. Go to the **VMS Servers** tab
2. Open **Alarms**
3. Click **New Alarm**



4. Enter all needed information in the **General** tab

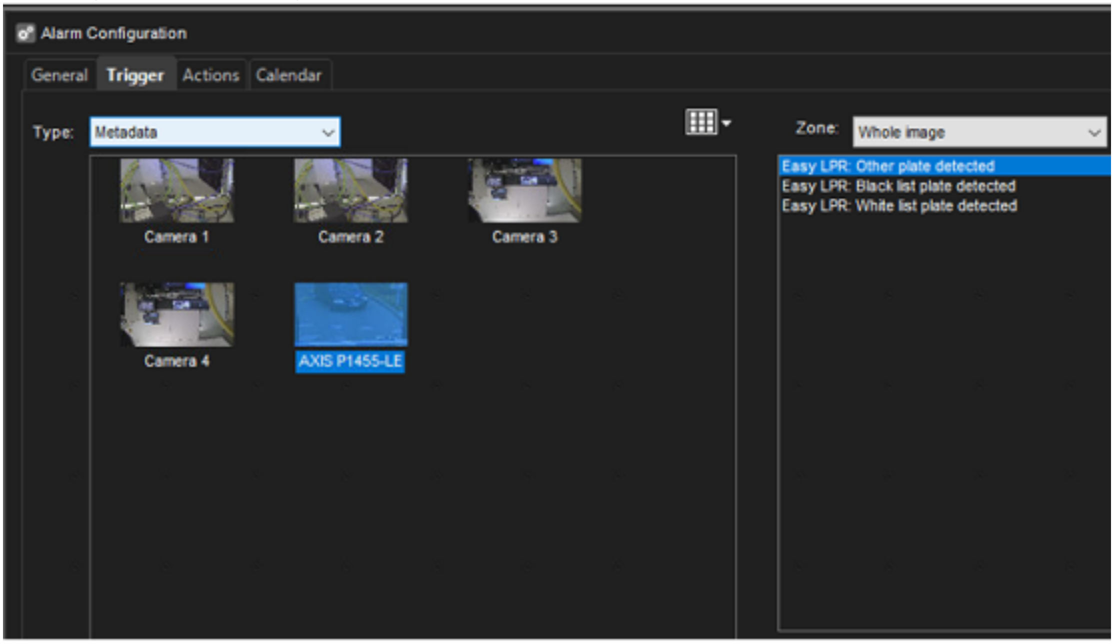
5. Open **Trigger** tab

6. Select trigger type **Metadata**

7. Select LPR camera

8. Select correct event:

- **Easy LPR: Other plate detected**
- **Easy LPR: Black list plate detected**
- **Easy LPR: White list plate detected**


Alarm Configuration

General | Trigger | Actions | Calendar

Type: Metadata

Zone: Whole image

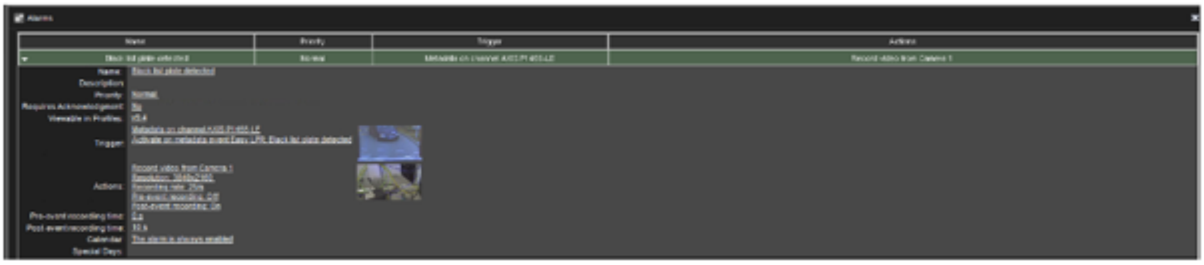
Easy LPR: Other plate detected
Easy LPR: Black list plate detected
Easy LPR: White list plate detected

9. Enter the actions of the alarms

10. Set calendar

11. Check overall view of the alarm

12. Click **OK** to confirm an alarm creation



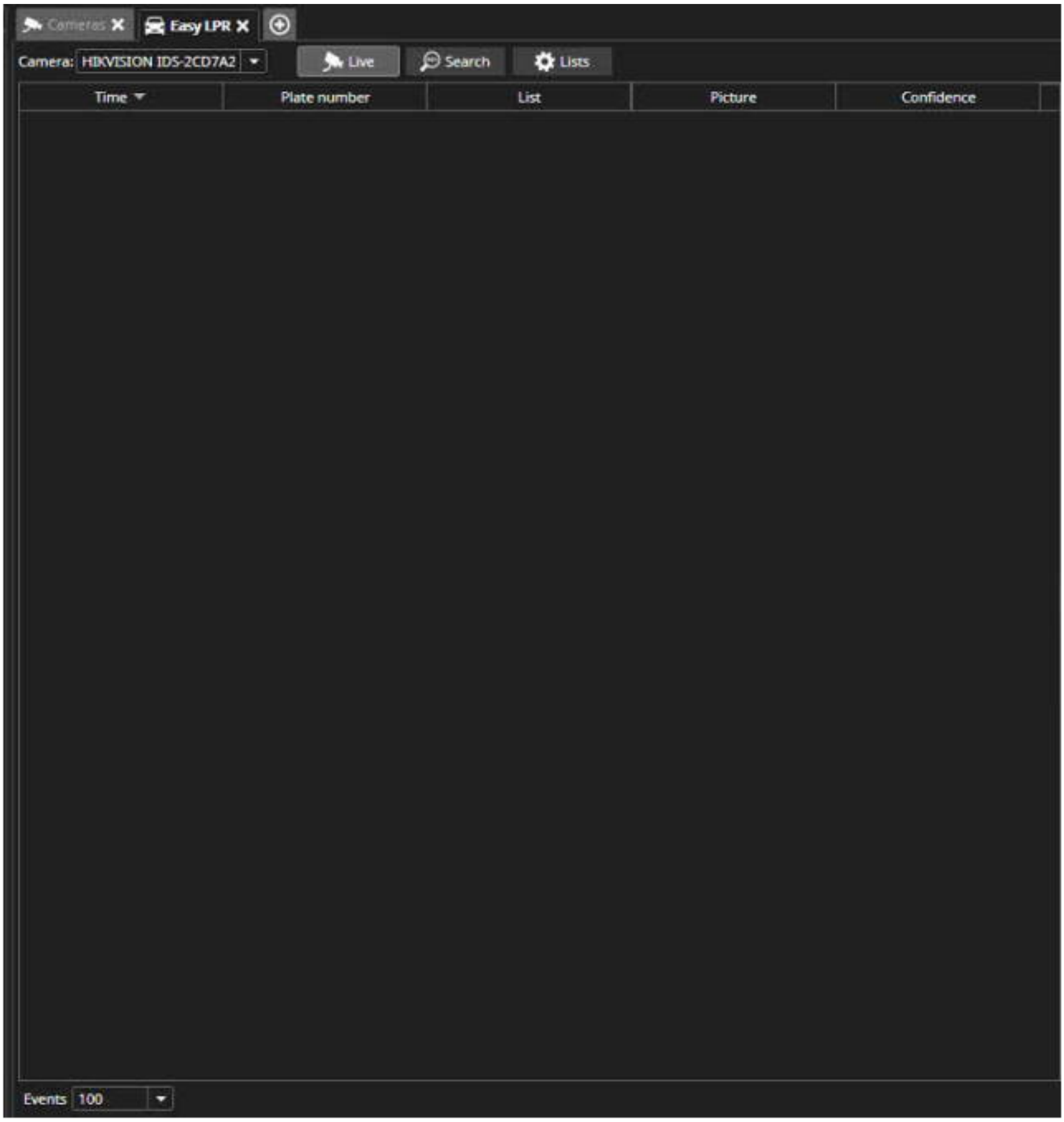
Name	Priority	Trigger	Actions
Black list plate detected	Normal	Metadata on channel AXIS P1455-LE	Record video from Camera 1

Name:	Black list plate detected
Description:	
Priority:	Normal
Requires Acknowledgement:	No
Viewable in Profiles:	v5.4
Trigger:	Metadata on channel AXIS P1455-LE Activate on metadata event Easy LPR: Black list plate detected
Actions:	Record video from Camera 1 Resolution: 3840x2160 Recording rate: 25/s Pre-event recording: Off Post-event recording: On
Pre-event recording time:	5 s
Post-event recording time:	10 s
Calendar:	The alarm is always enabled
Special Days:	

Using Easy LPR

Easy LPR contains the following functionalities:

- Live monitoring from the 1 camera at the same time
- The search of the number plates
- Lists Management
- Digital output controlling based on lists

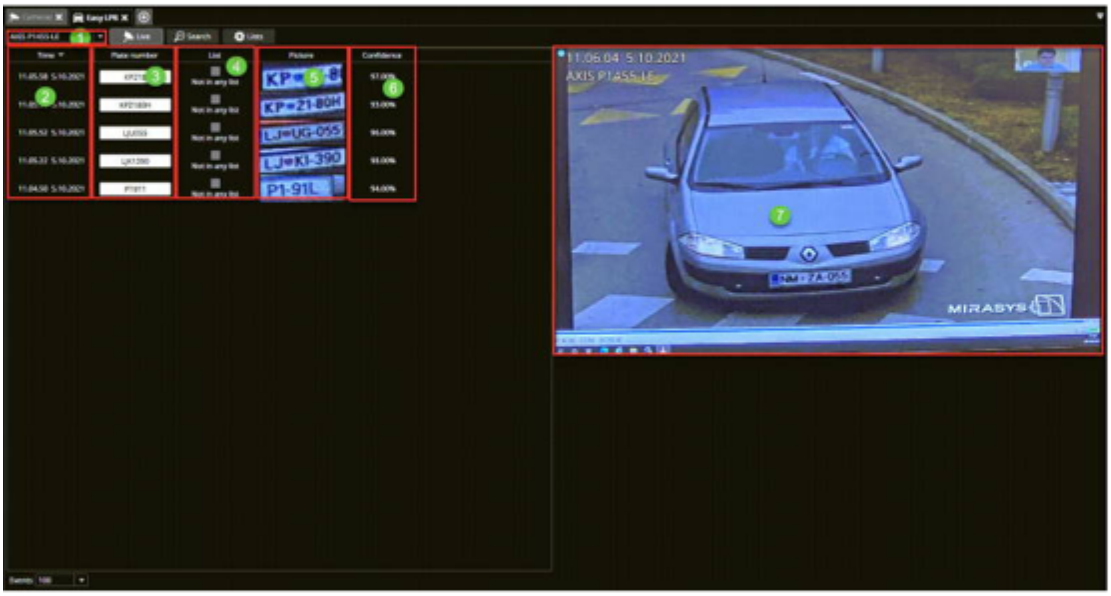


Live

The live tab shows the following information:

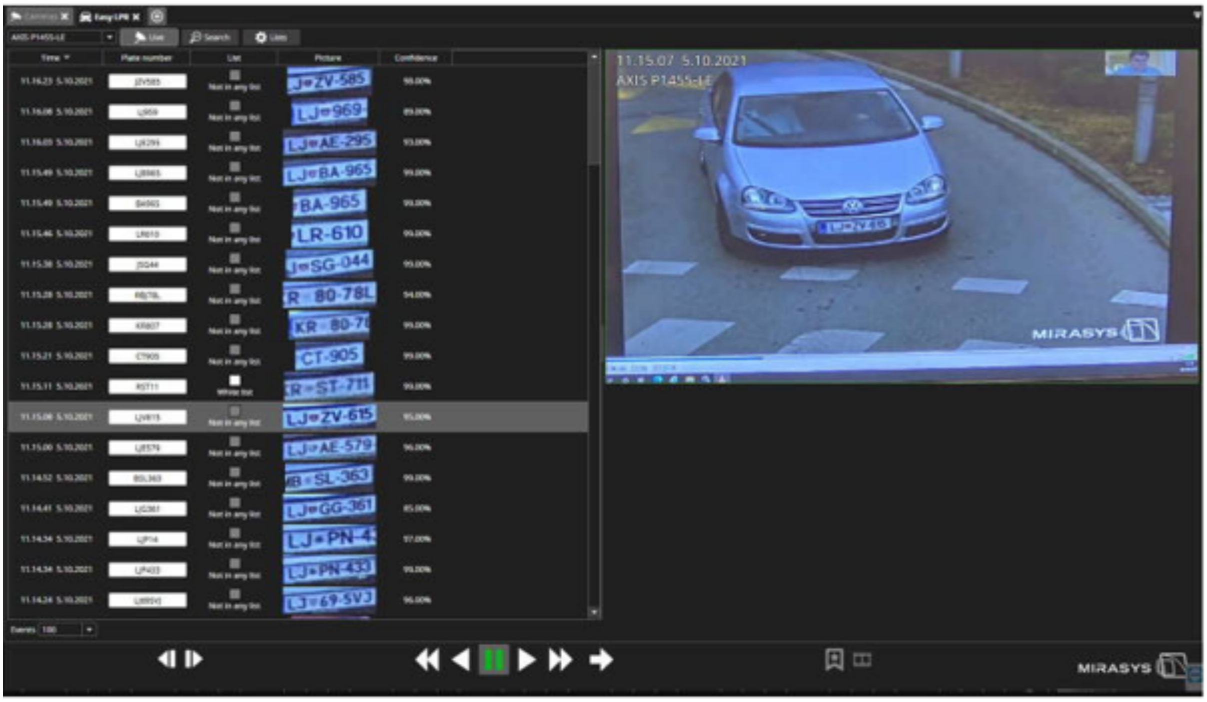
- The selection of the LPR camera
- Time of the plate detection

- Plate number
- Plate list
- Picture of the plate number
- Confidence of the plate reading
- Live view from the LPR camera



Time ▼	Plate number	List	Picture	Confidence
11.05.58 5.10.2021	KP21[illegible]	Not in any list	KP 8	97.00%
11.0[illegible] 5.10.2021	KP2180H	Not in any list	KP 21-80H	93.00%
11.05.52 5.10.2021	LJUG55	Not in any list	LJ UG-055	96.00%
11.05.22 5.10.2021	LJK1390	Not in any list	LJ KI-390	93.00%
11.04.50 5.10.2021	P191I	Not in any list	P1-91L	94.00%

When the plate information is clicked by the mouse, then the view changes to the playback mode and show the recorded situation.



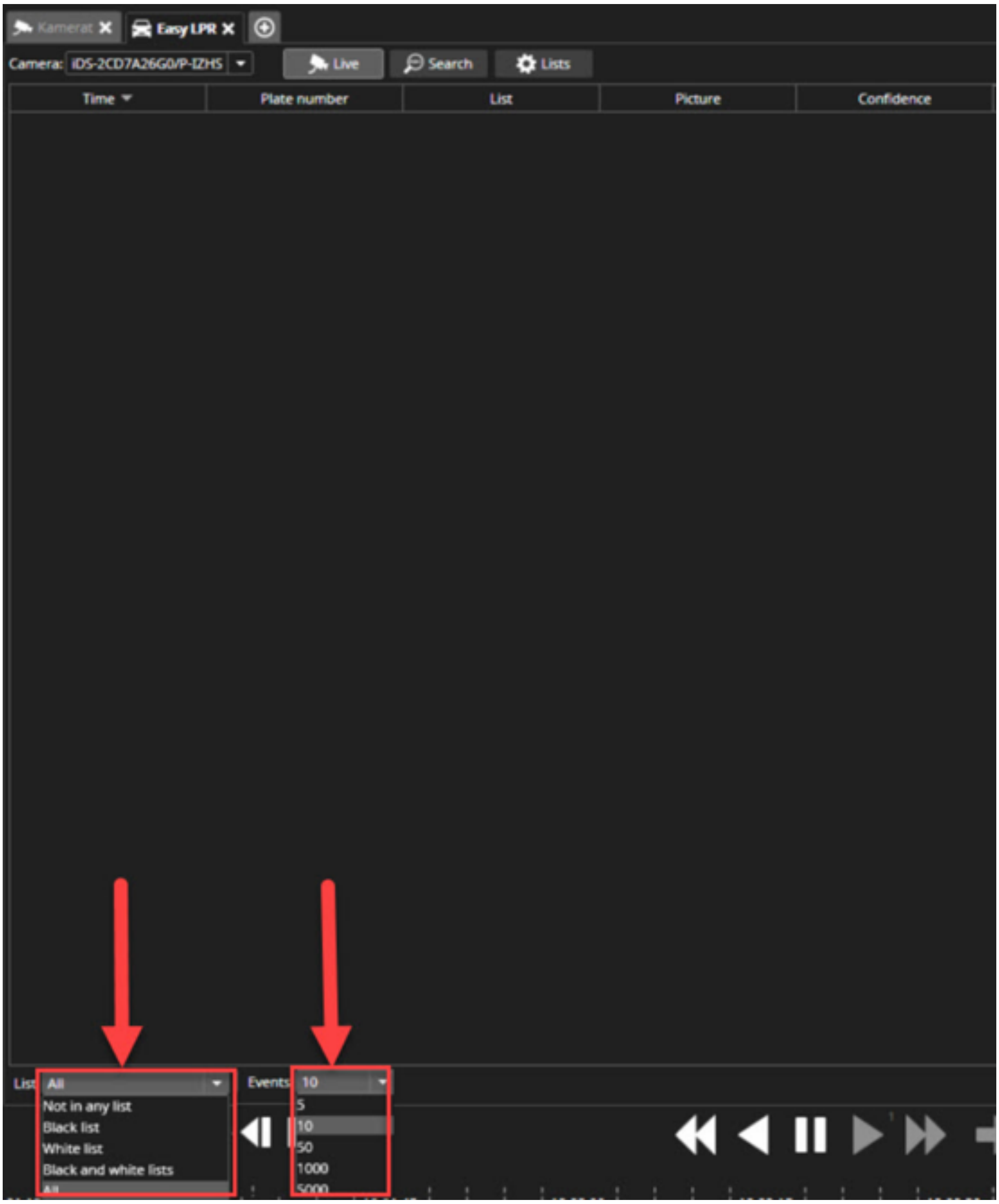
Filtering the Live view (supported since V9.5.0)

The user can which list are shown in the Live view. Options are:

- All
- Not in any list
- Black list
- White list
- Black list and White list

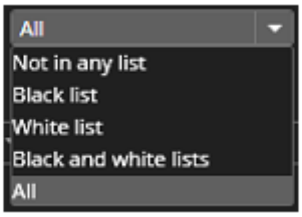
The user can set the amount of the result in the Live view. Options are:

1. 5, 10, 50, 1000 and 5000

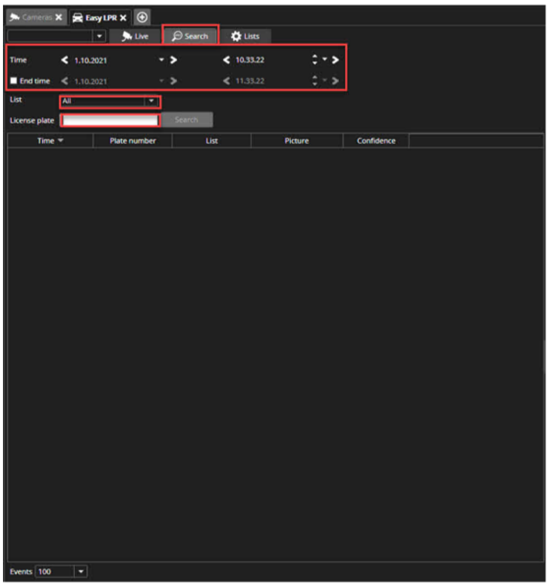

Kamerat
Easy LPR
Camera: iDS-2CD7A26G0/P-IZHS
Live
Search
Lists
Time
Plate number
List
Picture
Confidence
List
All
Not in any list
Black list
White list
Black and white lists
All
Events
10
5
10
50
1000
5000

Searching License plates

- Open **Search** tab
- Select LPR camera from the upper left corner
- Select time and date
- Enter **End time**, if needed
- Select list for the search
    - All
    - Not in any list
    - Black list
    - White list
    - Black and white list



1. Enter license plate(partial information is also accepted)
2. Click **Search**



Time 1.10.2021 10.33.22

□ End time 1.10.2021 11.33.22

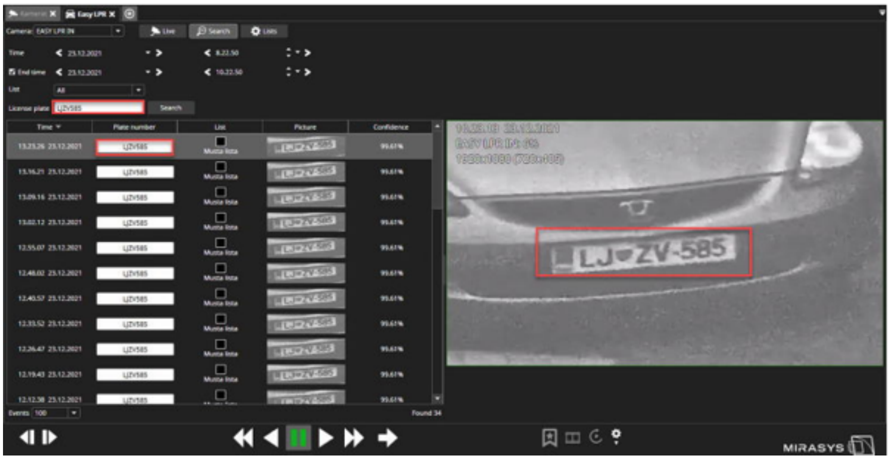
List All

License plate

Time	Plate number	List	Picture	Confidence

Events 100

Search will show all results. The user can playback selected time and use all normal playback functions.



Time 23.12.2021 8.22.50
☑ End time 23.12.2021 10.22.50
List All
License plate LJZV585

Time	Plate number	List	Picture	Confidence
13.23.26 23.12.2021	LJZV585	■ Musta lista	LJ ZV-585	99.61%
13.16.21 23.12.2021	LJZV585	■ Musta lista	LJ ZV-585	99.61%
13.09.16 23.12.2021	LJZV585	■ Musta lista	LJ ZV-585	99.61%
13.02.12 23.12.2021	LJZV585	■ Musta lista	LJ ZV-585	99.61%
12.55.07 23.12.2021	LJZV585	■ Musta lista	LJ ZV-585	99.61%
12.48.02 23.12.2021	LJZV585	■ Musta lista	LJ ZV-585	99.61%
12.40.57 23.12.2021	LJZV585	■ Musta lista	LJ ZV-585	99.61%
12.33.52 23.12.2021	LJZV585	■ Musta lista	LJ ZV-585	99.61%
12.26.47 23.12.2021	LJZV585	■ Musta lista	LJ ZV-585	99.61%
12.19.43 23.12.2021	LJZV585	■ Musta lista	LJ ZV-585	99.61%
12.12.38 23.12.2021	LJZV585	■	LJ ZV-585	99.61%

Lists

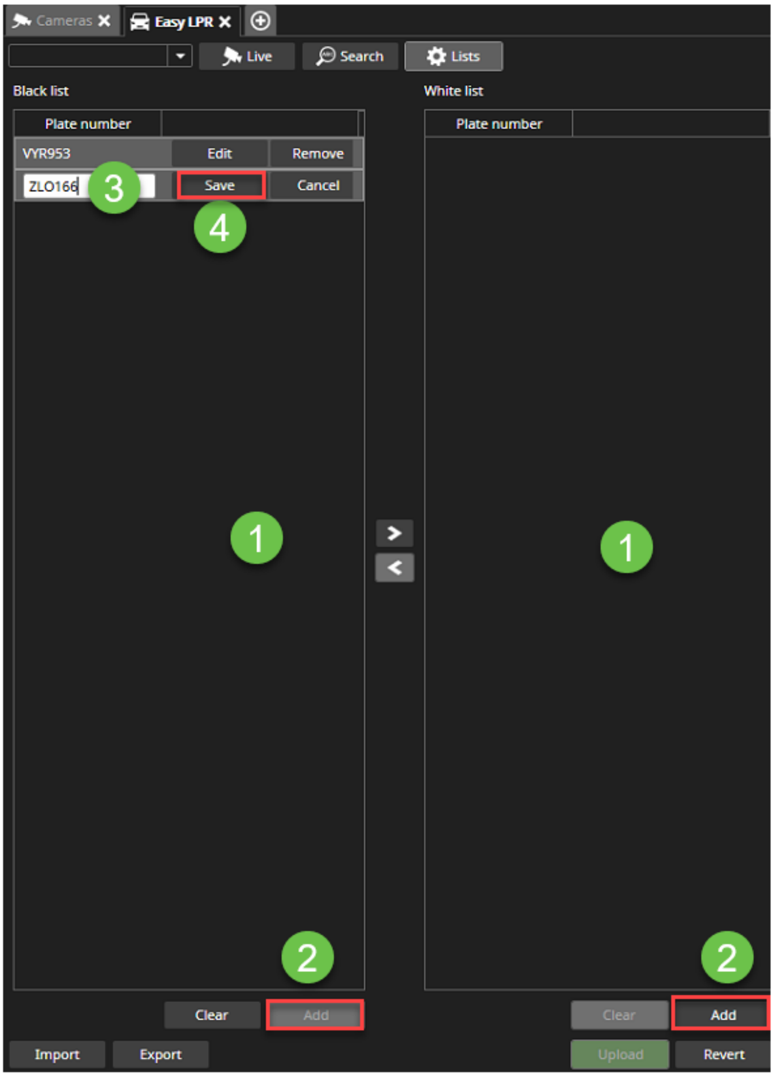
With the Easy LPR Lists Management, the users can do the following actions:

1. Add plate number
2. Edit plate numbers
3. Move plate numbers between the lists
4. Export plate numbers from the Spotter to the PC(**CSV**)
5. Import edited plate number lists to the Spotter
6. Upload lists from the Spotter to the LPR cameras

Please remember to upload lists to the cameras after any change.

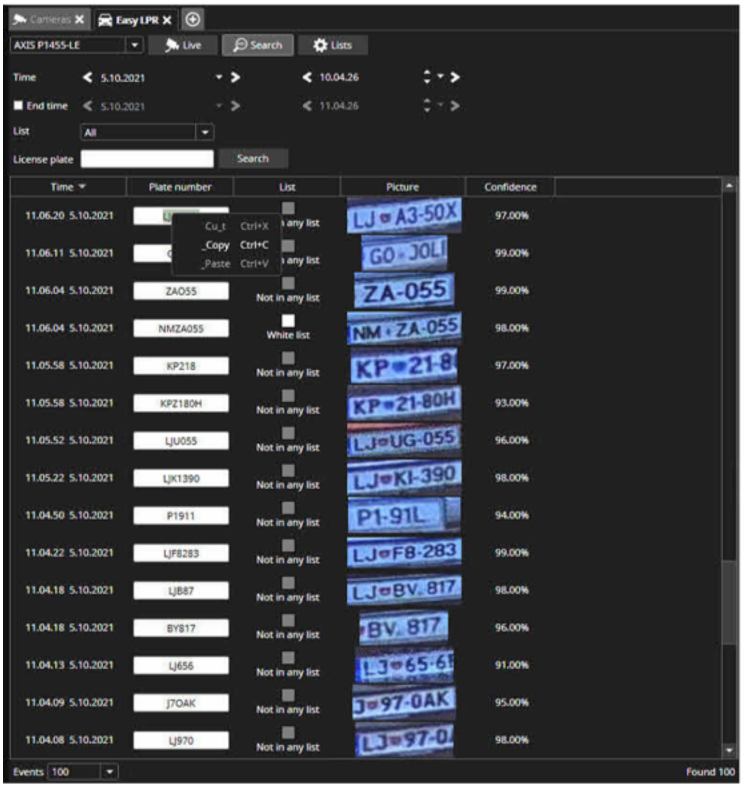
Adding Plate number

1. Select the **Black list** or **White list**
2. Click **Add**
3. Type the plate number
4. Click **Save**



Adding plate number from the search view

- Double-click plate number field
- Right mouse click top of the plate number
- Click **Copy**



Time 5.10.2021 10.04.26

□ End time 5.10.2021 11.04.26

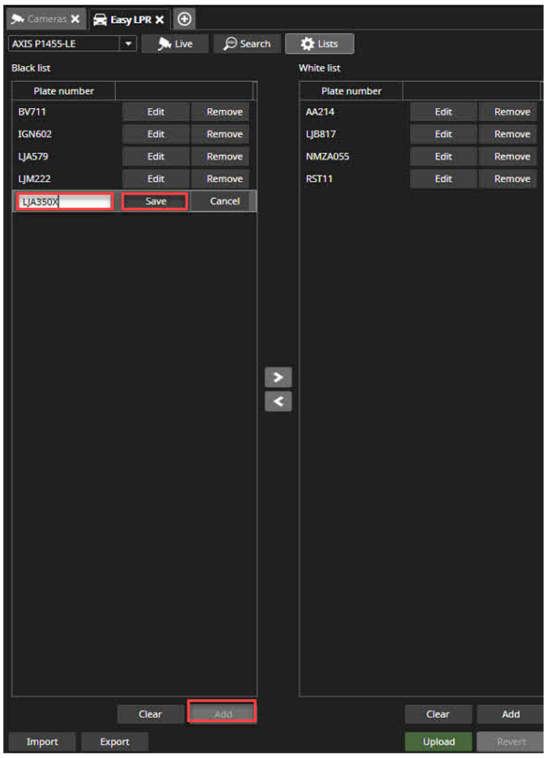
List All

License plate Search

Time	Plate number	List	Picture	Confidence
11.06.20 5.10.2021	LJ	any list		97.00%
11.06.11 5.10.2021	G	any list		99.00%
11.06.04 5.10.2021	ZAO55	Not in any list		99.00%
11.06.04 5.10.2021	NMZA055	White list		98.00%
11.05.58 5.10.2021	KP218	Not in any list		97.00%
11.05.58 5.10.2021	KPZ180H	Not in any list		93.00%
11.05.52 5.10.2021	LJU055	Not in any list		96.00%
11.05.22 5.10.2021	LJK1390	Not in any list		98.00%
11.04.50 5.10.2021	P1911	Not in any list		94.00%
11.04.22 5.10.2021	LJF8283	Not in any list		99.00%
11.04.18 5.10.2021	LJB87	Not in any list		98.00%
11.04.18 5.10.2021	BY817	Not in any list		96.00%
11.04.13 5.10.2021	LJ656	Not in any list		91.00%
11.04.09 5.10.2021	J7OAK	Not in any list		95.00%
11.04.08 5.10.2021	LJ970	Not in any list		98.00%

Events 100 Found 100

- Open **Lists**
- Select current list
- Click **Add**
- Paste plate number
- Click **Save**



Black list

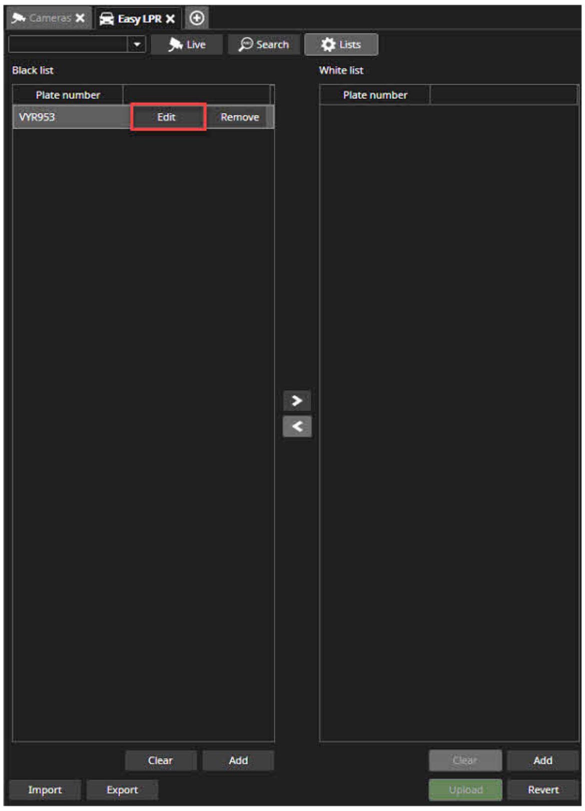
Plate number		
BV711	Edit	Remove
IGN602	Edit	Remove
LJA579	Edit	Remove
LJM222	Edit	Remove
LJA350X	Save	Cancel

White list

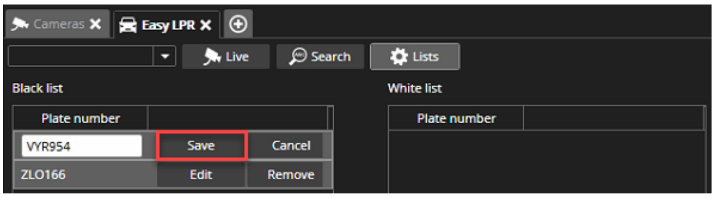
Plate number		
AA214	Edit	Remove
LJB817	Edit	Remove
NMZA055	Edit	Remove
RST11	Edit	Remove

Editing Plate Number

1. Select the plate number
2. Click **Edit**

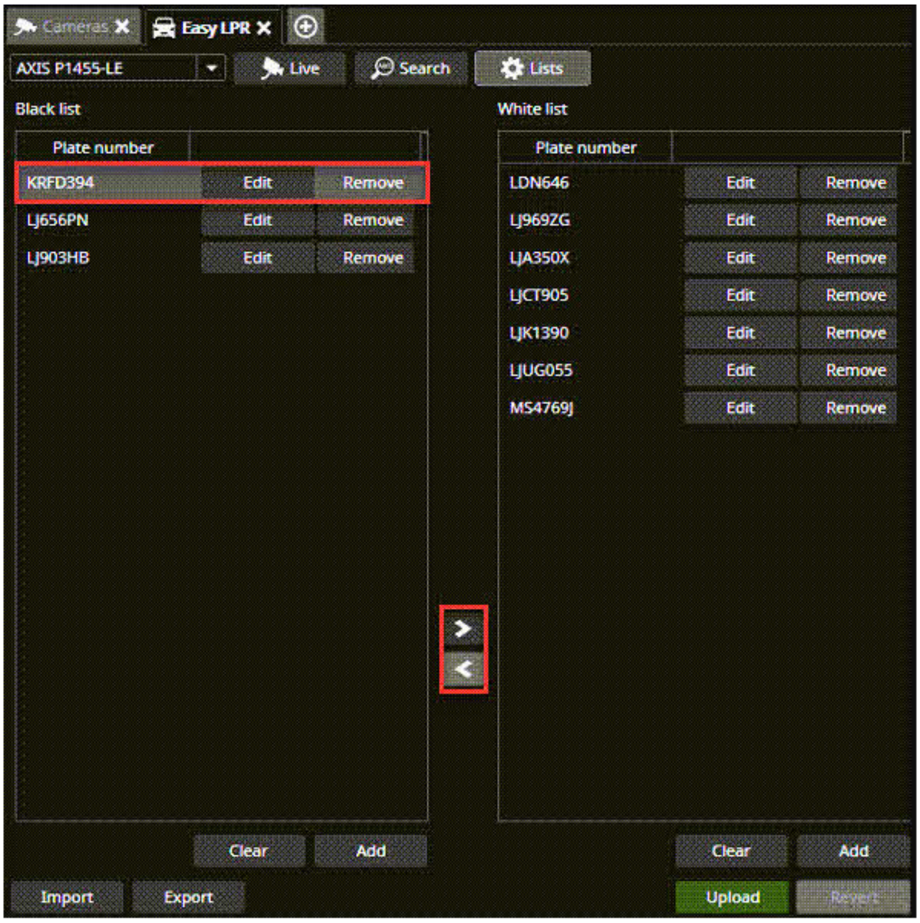


3. Do the modification and click **Save**



Moving Plate Number between the lists

1. Select the plate number from the list
2. Click arrow to move needed list



Black list

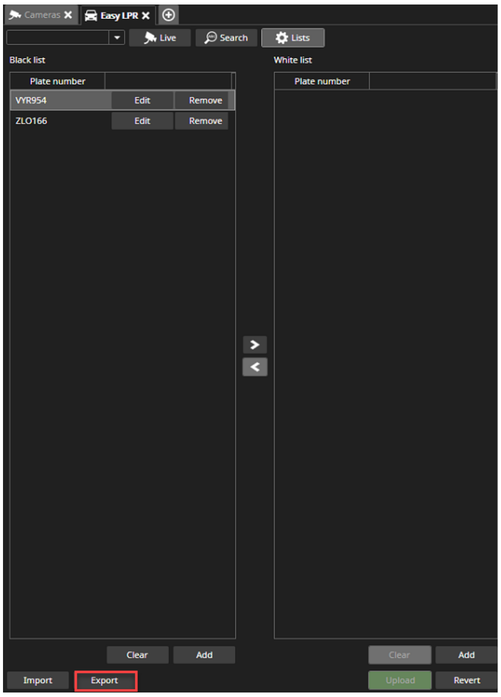
Plate number		
KRFD394	Edit	Remove
LJ656PN	Edit	Remove
LJ903HB	Edit	Remove

White list

Plate number		
LDN646	Edit	Remove
LJ969ZG	Edit	Remove
LJA350X	Edit	Remove
LJCT905	Edit	Remove
LJK1390	Edit	Remove
LJUG055	Edit	Remove
MS4769J	Edit	Remove

Export Plate Number lists

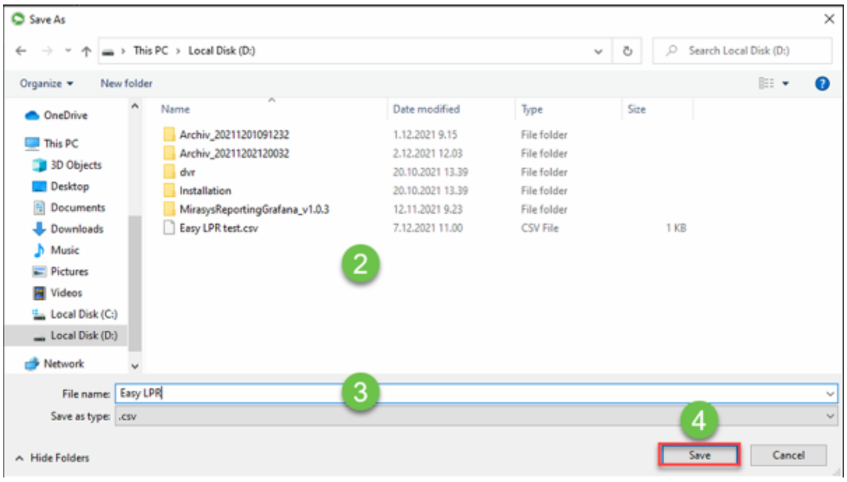
1. Click **Export**



2. Define the destination folder

3. Set the file name(.csv)

4. Click **Save**



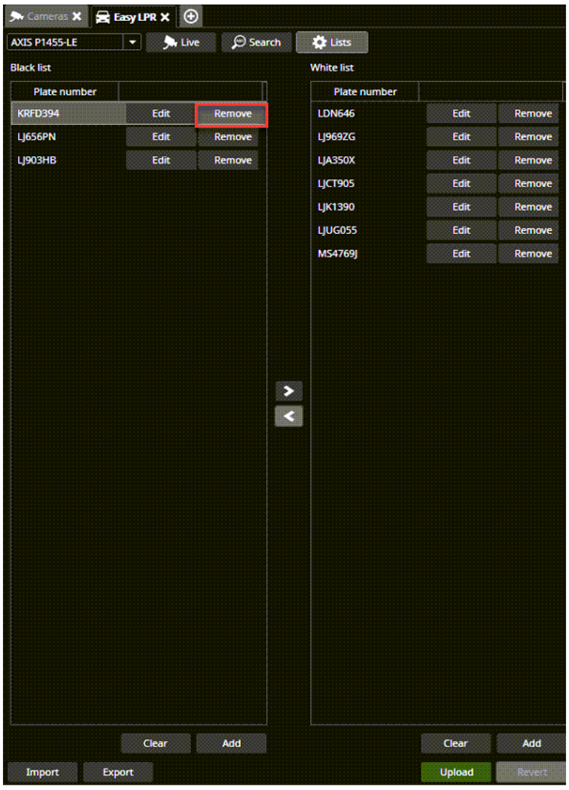
Name	Date modified	Type	Size
Archiv_20211201091232	1.12.2021 9.15	File folder	
Archiv_20211202120032	2.12.2021 12.03	File folder	
dvr	20.10.2021 13.39	File folder	
Installation	20.10.2021 13.39	File folder	
MirasysReportingGrafana_v1.0.3	12.11.2021 9.23	File folder	
Easy LPR test.csv	7.12.2021 11.00	CSV File	1 KB

File name: Easy LPR

Save as type: .csv

Removing Plate Numbers

1. Select the plate number from the list
2. Click Remove



Black list

Plate number		
KRFD394	Edit	Remove
LJ656PN	Edit	Remove
LJ903HB	Edit	Remove

White list

Plate number		
LDN646	Edit	Remove
LJ969ZG	Edit	Remove
LJA350X	Edit	Remove
LJCT905	Edit	Remove
LJK1390	Edit	Remove
LJUG055	Edit	Remove
MS4769J	Edit	Remove

With the import, the user can import a large number of plate numbers at the same time

1. Open exported CSV file

CSV content is shown below:

Plate number, List (1 = black list / 2 = white list)

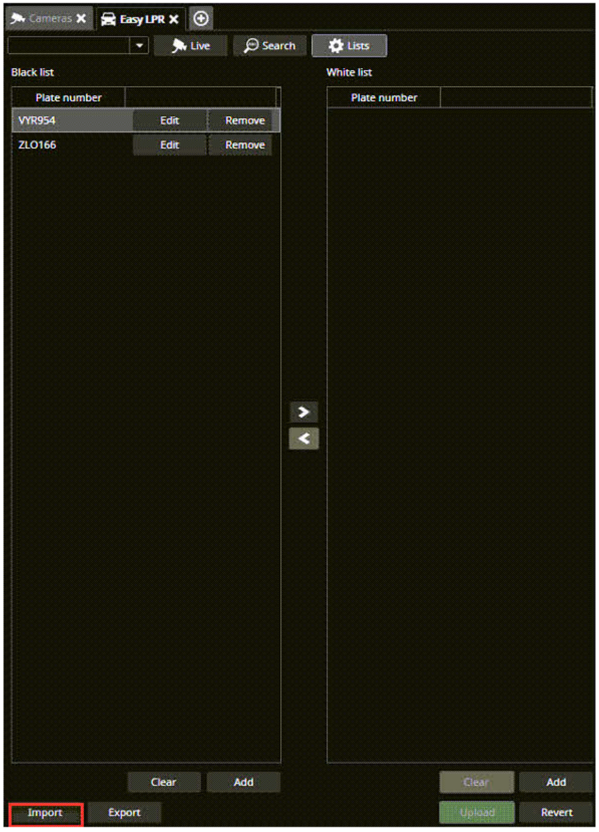
LJ656PN,1

LJ731CV,1

LJZV585,1

LJZV584,2

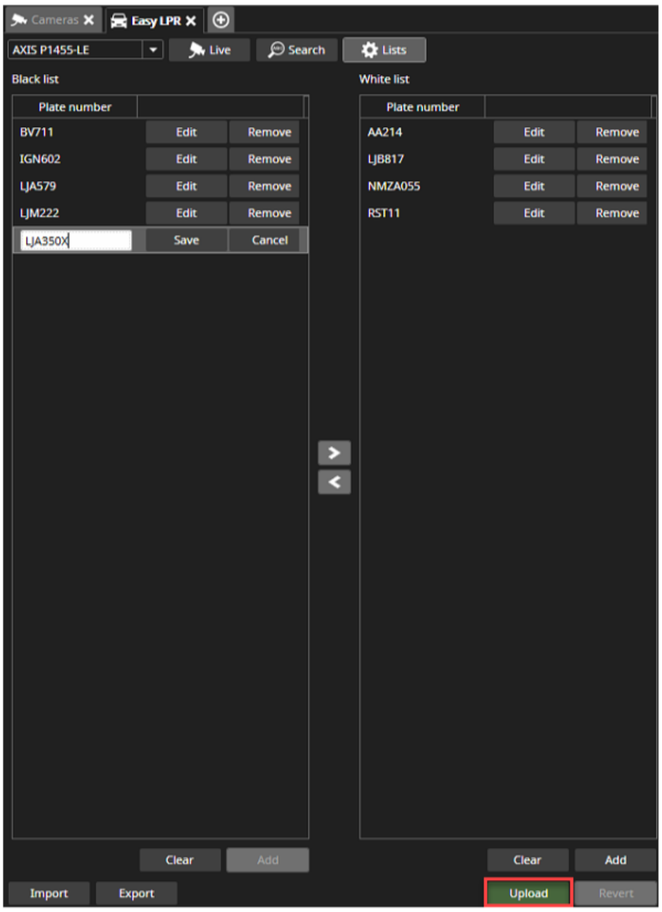
1. Add a new line with format ZLO166,2 for each new plate number
2. Select correct list(**List 1 = Black list, List 2 = White List**)
3. Save changes
4. Click **Import**



5. Browse to the location of the CSV file
6. Select the file and click **Open**

With the upload, the user can upload created black & white lists to the camera

1. Select camera, which list will be uploaded
2. Click **Upload**



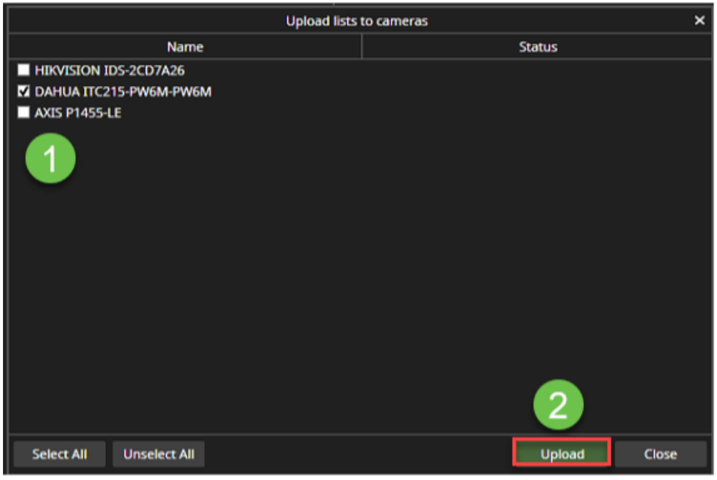
Black list

Plate number
BV711
IGN602
LJA579
LJM222
LJA350X

White list

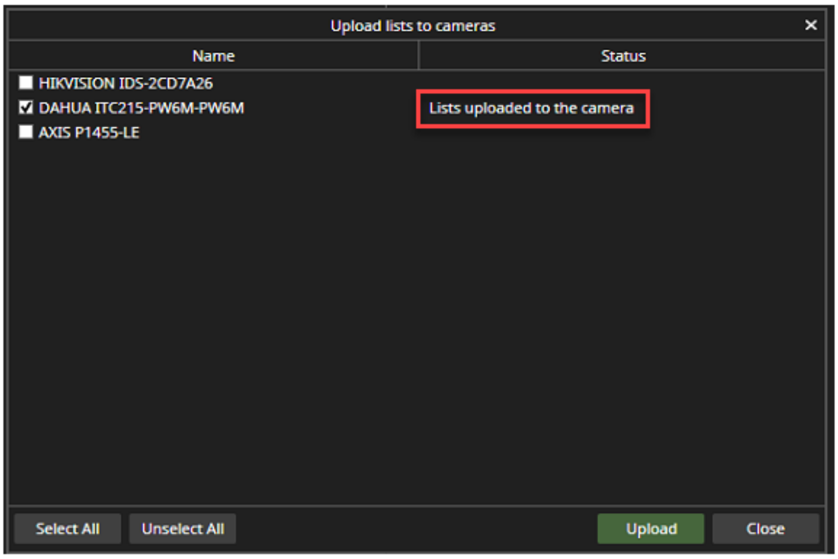
Plate number
AA214
LJB817
NMZA055
RST11

1. Select cameras, where lists are uploaded
2. Click **Upload**



Name	Status
□ HIKVISION IDS-2CD7A26	
☑ DAHUA ITC215-PW6M-PW6M	
□ AXIS P1455-LE	

After the upload, the status field shows information **List uploaded to the camera**



Upload lists to cameras

Name	Status
□ HIKVISION IDS-2CD7A26	
☑ DAHUA ITC215-PW6M-PW6M	Lists uploaded to the camera
□ AXIS P1455-LE	

Mirasys List Management (LM)

List Management (LM) is used to process Face Recognition (FR) and License Plate Recognition (LPR) events by matching detected faces and license plates to an identity and identity list. LM service is used to store identities and identity list information, receive and save LPR and FR events, send LPR and FR events to clients, do searches in saved events, and send LPR and FR events to the VMS server for processing.

LM service has the following abilities:

- Store identities and identity lists in the database
- Receive and store LPR and FR events in the database
- Match detected license plates and faces to defined identities and identity lists
- Search LPR and FR events from the database using search parameters
- Send real-time LPR and FR events for clients and recorders
- Send LPR and FR events to the VMS server for processing
- Notify clients and recorders about changes in identities and identity lists
- Enable integration to License Plate and Face recognition

The list Management service has a separate installer, so it can execute on a separate server or on some VMS server.

List Management settings (identities and identity lists) can be managed in System Manager List Management settings and in the Spotter Smart List Management plugin.